Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas

Implementación de una solución de seguridad informática bajo la plataforma de gestión unificada de amenazas

Caso: Municipalidad de Miraflores

TESINA

Para optar el Título Profesional de Ingeniera de Sistemas

AUTOR

Ennia CABALLA TORRES

William Leonardo TORRES FLORES

ASESOR

Juan Carlos GONZALES SUÁREZ

Lima, Perú

2010

Referencia bibliográfica

Caballa, E. & Torres W. (2010). *Implementación de una solución de seguridad informática bajo la plataforma de gestión unificada de amenazaz. Caso: Municipalidad de Miraflores*. Tesina para optar el título profesional de Ingeniero de Sistemas. Escuela Académica Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

Dedicatoria

A nuestros padres por su incansable, ilimitado apoyo y amor incondicional a lo largo de todas nuestras vidas, y por ser hoy lo que somos gracias a ellos.

Agradecimientos

A nuestro asesor, el profesor Juan Carlos Gonzales, quien nos guío y orientó en la elaboración de esta tesina.

Al ingeniero Luis Francisco Sierra, administrador de red de la Municipalidad de Miraflores, por las facilidades brindadas para el desarrollo de este trabajo.

A Cristian Carrión Morales por la colaboración brindada durante la elaboración de la tesina, por toda la paciencia y confianza.

Al Ingeniero José Luis Yucra Tomaylla por brindarnos su amistad y apoyo en todo momento.

A mi amigo Percy Canchan por brindarnos su apoyo, ánimo y colaboración cuando más se necesitaba.

RESUMEN

IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD INFORMÁTICA BAJO LA PLATAFORMA DE GESTION UNIFICADA DE AMENAZAS

ENNIA CABALLA TORRES
WILLIAM TORRES FLORES

Asesor: Juan Carlos Gonzales Suarez
Catedrático de la Facultad de Ingeniería de Sistemas y Informática

---

En la actualidad, los incidentes de seguridad informática en las empresas continúan aumentando al igual que el riesgo de ataques futuros. Con la evolución de amenazas mediante ataques múltiples y combinados (virus, gusanos, y vulnerabilidades), que fueron diseñados para maximizar el daño, se desarrollo soluciones puntuales originando el incremento de la complejidad de la red y sus administración también se volvió engorroso.

En la presente tesina, pretende dar a conocer la problemática que se enfrentan las organizaciones con respecto a la seguridad informática, como se resume en el párrafo anterior, frente a esto se brinda una alternativas de solución basados en la implementación de dispositivos UTM, la cual es un equipo optimizado y diseñado para realizar trabajos exclusivos de firewall y servicios adicionales tales como IDS/IPS, antivirus, antispam, VPN y filtro de contenidos.

Como toda la seguridad de la red se centralizará en un solo equipo especializado. La organización debe prever cualquier fallo del equipo por tanto es indispensable implementar un clúster de alta disponibilidad para superar esta vulnerabilidad para garantizar el funcionamiento ininterrumpido del equipo.

A través de un caso práctico aplicado en la municipalidad de Miraflores, donde se evaluó la situación y la problemática. Se presentó tres alternativas de solución basada en la

implementación de dispositivos UTM, en base a una tabla de puntajes y los requerimientos técnicos, se seleccionó la alternativa ganadora y se implementó la solución.

La conclusión más resaltante que se pretende evidenciar con el presente trabajo de investigación es demostrar que mediante una implementación de una solución de seguridad informática basada en tecnología UTM se simplificará y centralizará la administración de la seguridad así también se mejorará capacidad de detección y reacción ante problemas.

Palabras Claves: Dispositivos UTM, Clúster de alta Disponibilidad, IDS/IPS, filtro de contenido, antispam, antivirus, firewall, seguridad informática.

ABSTRACT

IMPLEMENTATION OF AN INFORMATION SECURITY SOLUTION UNDER THE PLATFORM FOR UNIFIED THREAT MANAGEMENT

ENNIA CABALLA TORRES
WILLIAM TORRES FLORES

Adviser: Juan Carlos Gonzales Suarez
University professor of Faculty Engineering of Systems and Informatics

---

Nowadays, computer security incidents in companies continue to increase as the risk of future attacks. With the evolution of threats through multiple and combined attacks (viruses, worms, and vulnerabilities), which they were designed to maximize the damage, developing specific solutions causing increased network complexity and management became too difficult.

In the present investigation work , to make known the problems faced by organizations with regard to computer security, as summarized in the preceding paragraph, therefore it provides three alternatives based on the implementation of UTM appliances, which are optimized and designed equipment for exclusive works firewall and additional services such as IDS / IPS, antivirus, antispam, VPN and content filtering.

As all network security will be centralized in specialized equipment. The organization has to provide any equipment failure therefore it is essential to implement a high availability cluster to overcome this vulnerability to ensure uninterrupted operation of the equipment.

Through a case study implemented in the municipality of Miraflores, it assessed the situation and problems. It presented three alternative solution based on the implementation

of UTM devices, based on a scoreboard and the technical requirements, Winning the alternative was selected and implemented the solution.

The most remarkable conclusion that you want to prove with this research is to demonstrate that by implementing a computer security solution based on UTM technology that will simplify and centralize management and security will also improve ability to detect and react to problems.

Keywords: UTM devices, high-availability cluster, IDS / IPS, content filtering, antispam, antivirus, firewall, computer security.

INTRODUCCION

La presente tesina se enfocará en la implementación de una solución de seguridad informática bajo la plataforma de gestión de amenazas unificadas con el objetivo de mejorar la seguridad informática a través de equipos optimizados, dispositivos UTM, para realizar trabajos exclusivos de firewall, especialmente el filtrado de paquetes, sistemas de detección y prevención de intrusos, antivirus, filtro de correo "basura", Filtro de contenidos y control del tráfico de red. Esta solución brinda grandes ventajas: reducirá el número de fabricantes y dispositivos integrados de seguridad, simplificará la administración de la seguridad, coordinará alertas, bitácoras y reportes y mejorará la capacidad de detección y reacción ante problemas.

En el capítulo I, se delinean los antecedentes del problema, la justificación, la delimitación y los objetivos de la presente tesina.

En el capítulo II, se describe el marco teórico, revisaremos temas como seguridad Informática, Principios Fundamentales de la seguridad informática, las amenazas lógicas como los principales tipos de ataques informáticos, fases del ataque informático. A demás se detallará todo sobre la tecnología UTM, sus antecedentes, Funcionamiento, los servicios de seguridad que dispone. También se ahondará las siguientes funciones del dispositivo UTM: Sistema de Detección de intrusión y sistema de Prevención de intrusión, Calidad de Servicio y clúster de alta disponibilidad.

En el capítulo III, presentamos el estado del arte metodológico, ahondaremos en las últimas tendencias sobre la tecnología de dispositivos UTM en cuanto a hardware y software que existen hoy en día.

En el capítulo IV, Implementación tecnológica se presentará el caso práctico de la municipalidad de Miraflores donde se analizará la situación actual y la problemática. Posteriormente se plantearán tres alternativas de solución y se evaluará cuál de estas alternativas se adecúa mejor.

INDICE DE CONTENIDO

INDICE DE FIGURAS

LISTA DE TABLAS

CAPITULO I

PLANTEAMIENTO METODOLÓGICO

1.1 El problema

1.1.1 Realidad Problemática

En la actualidad para garantizar la seguridad informática se tiene el paradigma de implantar firewalls y con ello se resolvería el problema. Sin embargo la red de datos es cada vez más complicada de proteger, la integración de los sistemas actuales con Internet y la necesidad de movilidad y de obtención de resultados en el menor tiempo, provoca un desequilibrio entre la seguridad y la facilidad de uso. Por eso, crece la necesidad de contar con herramientas más avanzadas que permitan defenderse mejor frente a agresiones cada vez más especializadas y difíciles de detectar.

Por otro lado la evolución de amenazas mediante ataques múltiples y combinados (virus, gusanos, y vulnerabilidades), que fueron diseñados para maximizar el daño y la velocidad de la infección, ahora son una práctica común, por ejemplo la situación del Spam era originalmente una molestia, pero ahora se ha convertido en una preocupación, por tanto la seguridad tradicional no es suficiente.

Con el tiempo las soluciones de seguridad informática también evolucionaron y los fabricantes construyeron soluciones puntuales originando que el data center concentre mayor cantidad de equipos y con ello la administración descentralizada de la seguridad se volvió más compleja, costosa y mayor consumo energético.

1.1.2 Enunciado del Problema

El problema principal es la administración descentralizada de la seguridad informática que posee mayores probabilidades de riesgo.

1.1.2.1 Problema Especifico 1

¿En qué medida se puede controlar las amenazas de seguridad informática para reducir los tiempos de inactividad de los servicios de red?

1.1.2.2 Problema Específico 2

¿Qué acciones se pueden tomar para aumentar la disponibilidad de los equipos que administran la seguridad de la red ante un desperfecto o avería?

1.1.2.3 Problema Específico 3

¿En qué medida se puede optimizar el ancho de banda disponible para garantizar el funcionamiento de los servicios de red?

1.1.3 Delimitación de la investigación

1.1.3.1 Delimitación Espacial

El proyecto se ejecutó en la municipalidad de Miraflores localizado en la Av. Larco Nº 400 – Miraflores en el departamento de Lima.

1.1.3.2 Delimitación Temporal

La fecha de ejecución del proyecto se realizó desde noviembre del 2009 con una duración de 30 días. Además la investigación del proyecto se realizó como fecha de inicio febrero hasta abril del 2010.

1.1.3.3 Delimitación Social

- Investigador: Ennia Caballa Torres
  William Torres Flores

- Asesor: Juan Carlos Gonzales Suárez

- Jurados: Raúl Armas Calderón
  Angel Sumoso Huamani

- Personas de la organización:
  - Jefe de Informática de la Municipalidad de Miraflores.
  - Administrador de Red de la Municipalidad de Miraflores.

1.2 Tipo y nivel de investigación

Según el Formato para Evaluación de Proyecto de Tesina de la UNMSM se tienen los siguientes tipos de investigación:

( ) BASICA (Aumento de conocimiento Existente sobre el tema).

( ) ADAPTATIVA (Acondicionamiento de una técnica, método o estrategia existente)

(X) APLICATIVA (Utilización del conocimiento Existente para mejorar algo).

( ) EXPLORATORIA (análisis situacional, estudio de hechos históricos).

( ) IDEOLOGICA (estudios filosóficos, culturales).

( ) REVISION (búsqueda bibliográfica).

1.3 Antecedentes

Existe en el mercado una gran cantidad de casos de éxito de organizaciones que utilizan firewall bajo la plataforma de gestión de amenazas unificadas (UTM):

Caso de éxito 1: Municipalidad de MAIPU, - Santiago de Chile

Se implementó un servicio de gestión perimetral bajo la plataforma UTM, con múltiples servicios, donde se instaló en las oficinas del cliente, entregado de esta forma un perfil de servicio altísimo. La configuración de los servicios internos, podrán ser puestos con perfiles con QoS para mejorar la experiencia de los usuarios internos activando también los Servicios de Firewall, Filtro Web. IDS / IPS, VPN IPSec / SSL, Bloqueo de mensajería instantánea (IM) y control de protocolos peer to peer (P2P) entre otros, además de Antivirus y Antispam para Correo.

Con esta solución se resolvió varias debilidades que han sido detectadas en la red de la Municipalidad de MAIPU, además, de bajar los costos, por ejemplo:

- Centralizar y optimizar los recursos a través de una misma plataforma.
- Mantener una plataforma capaz de Gestionar diversos Servicios en línea.
- Ahorro en la capacidad de crecimiento a nivel de usuarios y de ancho de banda, sin necesidad de comprar licencias adicionales.

- Solución integral sobre un mismo Appliance con capacidad de Firewall, Antivirus, IDS / IPS, Traffic Shaping (QoS), Control de accesos contra fuga de información a través Mensajería Instantánea (IM), Control de descargas (Download).

Caso de éxito 2: Comparex España SA

Prestigiosa empresa de Servicios e integrador de Soluciones Tecnológicas con más de 30 años de experiencia en el mercado español y europeo.

Comparex España decidió implementar una solución integrada para proteger el correo corporativo frente a ataques y correos no deseados (spam, phishing, virus), filtrado web. Además Comparex requería de un servicio permanente, 24x7.

La plataforma y los servicios ofrecidos por una solución UTM permiten gestionar de forma integrada y eficiente los siguientes subsistemas:

- Capacidad de gestión de los correos entrantes y salientes de la organización
- Gestión del cumplimiento y la normativa de la compañía.
- Capacidad de Filtro Web.
- Gestión anti-spam.
- Gestión phishing (detección de fraude).
- Gestión Time Zero Virus.
- Ataques de directorio.
- Gestión virus.
- Control de Denegaciones de Servicio.
- Potente herramienta de gestión y reporte.
- Facilidad de implementación e instalación.
- Detección de zombie.

Mediante la implementación de una solución UTM se ha logrado una notable reducción de los ataques y correos no deseados como spam, phishing, virus, etc. Asimismo, Comparex España ha logrado implementar una normativa corporativa, un servicio permanente, 24x7, para agilizar tanto el tiempo como los costes de mantenimiento.

Caso de éxito 3: Ayuntamiento de Elda Valencia - España

Ofrece todos aquellos servicios necesarios para el ciudadano del término municipal de Elda, en la Comunidad Valenciana. Entre estos servicios se encuentran tramitaciones, información sobre subvenciones, becas, etc. Así como información sobre cultura, deportes, educación, fiestas, sanidad, transportes, entre otros, cubriendo todas las necesidades de sus ciudadanos y visitantes.

- El Ayuntamiento de Elda, teniendo en cuenta las necesidades de seguridad, que cada vez son más importantes, llevó a cabo una auditoría, que planteó las siguientes necesidades: Segmentar la red en VLAN´s por roles: Aislar los servidores y otros recursos críticos, así como gestionar el acceso a los mismos.
- Proteger la red de conexiones no autorizadas, tanto internas como externas.
- Proteger la red frente a la proliferación de virus y otras amenazas.
- Gestionar y controlar el acceso a determinadas páginas y aplicaciones.
- Posibilidad de conectar remotamente a los trabajadores móviles.
- Incorporar un sistema de WAN failover para asegurar el servicio de conectividad ante caídas de proveedores de servicio.
- Gestionar la solución de forma intuitiva.

A través de una solución UTM en HA implementada se logró satisfacer todas estas necesidades además aproximadamente 500 empleados del Ayuntamiento se han visto beneficiados, ya que todos y cada uno de los usuarios han de pasar por los dispositivos UTM de seguridad para acceder a recursos de otras zonas de la red.

En general el Ayuntamiento se ha visto beneficiado por el rendimiento, la flexibilidad y la potencia de estos dispositivos, y sobre todo, por el control total que tienen ahora sobre los accesos a los recursos críticos, previniendo cualquier tipo de ataque o infección a gran escala. Además el rendimiento de la red no se ha visto mermado en ningún momento.

1.4 Justificación

La gestión de seguridad informática con equipos de gestión de amenazas unificadas (UTM) permitirá:

a) Simplificar la administración de recursos de seguridad centralizando todo en sólo equipo.

b) Brindar una protección contra amenazas combinadas.

c) Controlar las amenazas basadas en contenido realizando una reconstrucción e inspección completa de contenidos comparándolos con firmas no autorizadas.

d) Brindar flexibilidad para proteger redes.

e) Reducir el costo de adquisición, licenciamiento y operación.

f) Reducir el consumo energético debido al empleo del menor número de equipos.

1.5 Objetivos

1.5.1 Objetivo General

Demostrar a través de un caso práctico que los equipos UTM simplificarán y mejorarán la administración de la seguridad informática.

1.5.2 Objetivos Específicos

1.5.2.1 Objetivo Especifico 1

Controlar las amenazas de seguridad informática para garantizar el funcionamiento de los servicios de red.

1.5.2.2 Objetivo Especifico 2

Aumentar la disponibilidad del equipo que administra la seguridad de la red ante un desperfecto o avería

1.5.2.3 Objetivo Especifico 3

Optimizar el ancho de banda disponible para garantizar el funcionamiento de los servicios de red

1.6 Hipótesis

1.6.1 Hipótesis general

Centralizando la administración de los servicios de red a través de equipos de gestión de amenazas unificadas (UTM) se mejorará la gestión de seguridad informática.

1.6.2 Hipótesis Específica

1.6.2.1 Hipótesis Específica 1

Controlando las amenazas de seguridad informática por medio de la implementación de un equipo UTM y configurando la función de los servicios de detección intrusos, prevención de intrusos, antivirus, antispam y filtro de contenido controlarán el funcionamiento de los servicios de red.

1.6.1.2 Hipótesis Específica 2

Implementando un sistema de alta disponibilidad tipo activo – pasivo para el equipo UTM que administra la seguridad de la red se reducirá el riesgo de tiempo de inactividad del mismo.

1.6.1.3 Hipótesis Específica 3

Optimizando el ancho de banda disponible por medio de la implementación del equipo UTM y configurando la función del servicio de control de tráfico (Traffic Shaping) para garantizar el desempeño de los servicios de red.

1.7 Recursos

1.7.1 Humanos

Los investigadores, el asesor y demás colaboradores de la municipalidad de Miraflores.

1.7.2 Materiales

Libros, revistas, artículos científicos e Internet. También se utilizó tesinas y tesis de maestría.

CAPITULO II

MARCO TEÓRICO

2.1 SEGURIDAD DE LA INFORMACIÓN

2.1.1 Introducción

Actualmente todas las empresas poseen Sistemas de Información (SI), los cuales contribuyen a la optimización del uso de las fuentes y los datos requeridos para su dirección. Los SI dotan a la empresa de la capacidad de comunicación y de análisis necesaria para desarrollar el negocio a un nivel de competencia cada vez más globalizado, el cual implica, muchas veces inteconexión con los proveedores y distribuidores, atención las 24 horas del día y dar servicio a las necesidades locales e internacionales.

Esta demanda – creciente año a año – de SI que soporten las complejas necesidades de comunicación e información de las empresas, afrontan un gran reto y al mismo tiempo un riesgo: "La Seguridad Informática".

Efectivamente, las empresas se están dando cuenta que tienen una gran infraestructura tecnologica que les agiliza sus procesos internos, pero que a su vez, representa un peligro por la vulnerabilidad que presenta ante un nuevo entorno de competencia.

Las Tecnologias de la Información y Computación (TIC) están dando nuevas soluciones a estos problemas, sin embargo debemos tener mucho cuidado de no cometer el error de comenzar a implementar soluciones que con el tiempo se vuelvan difíciles y complejas de administrar

2.1.2 Definición

La seguridad de la información es un índice que nos indica nuestra percepción del nivel de protección de nuestro de nuestro sistema informático, es decir que está libre de todo peligro, daño o riesgo.

No es posible lograr un 100% de seguridad pero nos podemos acercar en función de las medidas que implementemos

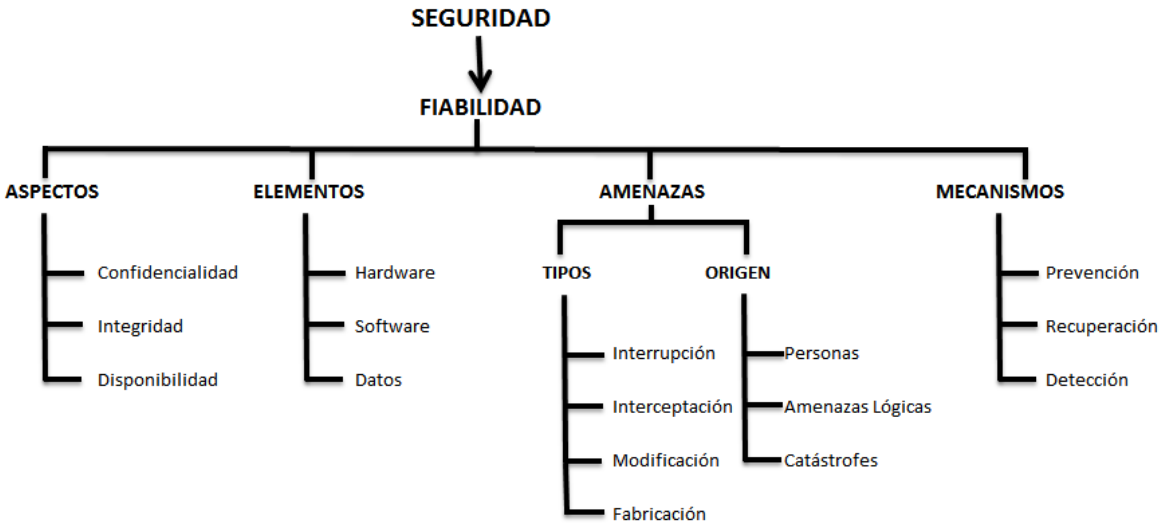


Figura 2.1 Visión Global de la Seguridad Informática

2.1.3 Principios fundamentales de Seguridad

Los tres principios fundamentales, los cuales indefectiblemente suelen encontrarse direccionados en todo programa integral de seguridad de la información, son conocidos individualmente como Confidencialidad, Integridad y Disponibilidad; y a menudo referidos en su conjunto como "CIA Triad" o "The Big Three".

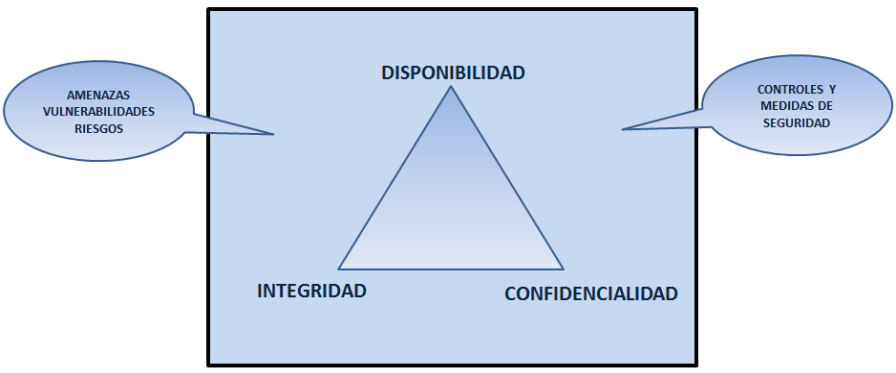


Figura 2.2 La triada CIA

2.1.3.1 Confidencialidad

El principio de Confidencialidad, asegura que el nivel necesario de secreto se encuentra asegurado en cada instancia del procesamiento de datos, de manera tal de prevenir su

divulgación a personas no autorizadas a conocer los mismos. Dicho de otro modo, la Confidencialidad de la Información, a menudo es referida como la necesidad de que la misma sólo sea conocida por personas autorizadas.

Varias son las amenazas que atentan contra la Confidencialidad: los usuarios pueden intencional o accidentalmente divulgar información sensible al no cifrar la misma antes de que esta sea enviada a otra persona, pueden ser víctima de algún tipo de ataque de ingeniería social en busca de secretos comerciales, información en tránsito puede ser interceptada por terceros que se encuentren en condiciones de realizar escuchas, etc.

La Confidencialidad, a menudo puede ser provista o reforzada, mediante la implementación de un estricto control de acceso, por medio de la encriptación de datos (ya sea al momento de almacenar o transmitir los mismos), la puesta en marcha de procesos de Clasificación de la Información, concientización y entrenamiento del personal. Cada uno de ellos suelen ser recursos de suma importancia a la hora de combatir efectivamente aspectos tales como la divulgación no autorizada.

2.1.3.2 Integridad

La Integridad de la Información es la característica que hace posible garantizar su exactitud y confiabilidad, velando por que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, de modo autorizado y mediante procesos autorizados. A su vez, es de suma importancia que esta modificación sea registrada para posteriores controles o auditorias.

Una falla de integridad puede estar dada entre otros, por anomalías en el hardware, software, virus informáticos y/o modificaciones inesperadas. Precisamente, a fin de mantener su integridad, el conjunto de hardware, software y mecanismos intervinientes en el tratamiento de la información, deben ser capaces de trabajar de manera coordinada, a efectos de procesar, mantener y mover los datos a su destino previsto, sin que los mismos sufran cualquier tipo de alteración inesperada.

Cuando un atacante distribuye un virus, una bomba lógica o un backdoor dentro del sistema, la integridad de este es comprometida. Este hecho puede afectar negativamente el principio de integridad de la información, debido a que la misma puede terminar por corromperse, ser contaminada mediante la introducción de datos erróneos/falsos o modificada con fines malévolos.

El control de acceso, los sistemas de detección de intrusos, la aplicación de chequeos de integridad, los procedimientos de control de cambios, la separación de funciones y la implementación del principio de "Menor Privilegio", son solo algunos de los medios utilizados para prevenir problemas de integridad.

2.1.3.3 Disponibilidad

La Disponibilidad u Operatividad de la Información es la capacidad de encontrarse siempre disponible, para ser utilizada por las personas autorizadas. A fin de cumplir con este principio, los sistemas y redes deben proveer la capacidad adecuada de procesamiento, actuar de modo previsible y brindar un adecuado nivel de performance. A su vez, ellos deberían ser capaces de recuperarse de interrupciones de manera rápida y segura, a fin de que la productividad no se vea afectada negativamente.

Entre las amenazas que afectan el principio de Disponibilidad, se encuentran las fallas relacionadas con el software y hardware, aspectos relacionados con el entorno (calor, frío, humedad, electricidad estática, etc.), desastres naturales, denegaciones de servicios (DoS, DDoS), etc.

A fin de prevenir inconvenientes que puedan afectar la Disponibilidad, deben ser implementados mecanismos de protección adecuados, tales como medidas de resguardo y recuperación, mecanismos redundantes, planes de contingencia, sistemas de prevención y/o detección de intrusos, procedimientos de hardening, etc

2.1.4 Amenazas a la seguridad

Las organizaciones, sus redes y sistemas de información enfrentan crecientes amenazas a su seguridad entre las cuales se incluyen: fraude asistido por computadora, actos de espionaje, sabotaje, vandalismo y hasta incendios e inundaciones.

En este contexto, amenaza puede ser definido como todo aquel evento cuya ocurrencia podría impactar en forma negativa en la organización.

En líneas generales, podemos realizar una clasificación de las amenazas según su origen, así encontramos entre otras las siguientes categorías:

- Amenazas físicas
- Catástrofes naturales
- Fraude informático
- Error humano
- Intrusiones
- Software ilegal
- Código malicioso

2.1.4.1 Tipos de Amenazas

• **Amenazas Físicas:** Se relacionan con la posibilidad de obtener acceso físico a los recursos. La mayoría de los sistemas de computación ha desarrollado altos niveles de sofisticación para cuidarse de las amenazas externas. Sin embargo, estos sistemas generalmente son vulnerables a ataques, sabotaje y robos originados en el interior. Existen varias medidas que se pueden implementar para mantener a los intrusos fuera del alcance de los recursos, por ejemplo, puertas, locks, sistemas de vigilancia y sistemas de alarma, junto con técnicas biométricas para el control de acceso al sistema.

• **Catástrofes Naturales:** Son aquellos desastres provocados por la naturaleza como los tornados, inundaciones, terremotos o fuertes tormentas eléctricas que pueden entre otras cosas, provocar interrupciones de servicio. Los desastres naturales ocasionan grandes pérdidas.

• **Fraude Informático:** Se refiere a las defraudaciones provocadas en el ámbito de empresas o en Internet. Se considera como tal, tanto al robo hormiga (Salami), como a la promoción de inversiones en sitios de Internet que nunca se concretan, la venta de productos y servicios informáticos que no existen y más recientemente el phishing.

• **Error humano:** Es aquel que se produce por impericia o negligencia y el alcance del mismo es, de hecho, impredecible. Entre los incidentes más comunes se cuentan: exposición de datos personales de clientes, olvido de hacer un backup o hacerlo mal, codificar aplicaciones con errores involuntarios que las hacen vulnerables, desconectar involuntariamente servidores que están brindando un servicio on-line, brindar información sobre la organización a personas desconocidas, elegir una contraseña fácilmente vulnerada u notarla en un lugar de fácil acceso porque no la puede recordar.

• **Intrusiones:** Las intrusiones son ingresos no autorizados a los sistemas de comunicaciones, servidores, estaciones de trabajo, quebrando la seguridad de la empresa u organización.

• **Software ilegal:** Los programas de computadoras están protegidos por las leyes de derechos de autor y por tratados internacionales. Mucha gente no tiene en cuenta que usar software copiado ilegalmente es un hurto y que el uso de software ilegal puede acarrear consecuencias serias a una organización, sus gerentes y sus empleados. Del mismo modo, la utilización de software ilegal a menudo puede terminar en la infección de virus u algún otro tipo de código malicioso.

• **Código Malicioso:** El código malicioso, es quizás la amenaza con mayor prensa y la más temida por todos los usuarios en general. Código malicioso es todo programa que genera algún tipo de problema en la computadora en la cual se ejecuta, ya sea robo o destrucción de información, pérdida de productividad, pérdida de privacidad, etc. Incluye a los virus, gusanos, caballos de Troya, espías, puertas traseras y software de control remoto subrepticio.

2.1.5 Hackers, Crackers y Script Kiddies

Mucho se ha escrito en la prensa acerca de los Hackers, y en rigor de verdad no todo lo que se lee en los periódicos es cierto. En el sentido si se quiere más romántico, un Hacker es aquella persona a la cual le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. Ellos ven el hacking, como un desafió intelectual. Así

mismo, con frecuencia se utiliza el neologismo “Hacker”, para referirse a un experto/gurú en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: (Programación, redes, sistemas operativos, hardware, etc.)

La historia de la informática y las comunicaciones, se encuentra llena de Hackers famosos, a quienes se les debe gran parte del desarrollo de la computación y las comunicaciones. Tim Vinton Cerf (inventor de los protocolos TCP/IP), Dennis Ritchie y Ken Thompson (Creadores de UNIX), Steve Jobs y Steve Wozniak (fundadores de Apple), Linus Torvalds (Desarrollador del primer kernel del sistema operativo GNU/Linux) y muchos otros.
Al margen de lo comentado y a nivel popular, en la actualidad el término Hacker suele ser utilizado para referirse a los intrusos informáticos, mientras que el termino Cracker suele utilizarse a efectos de identificar a aquellos hackers que utilizan su conocimiento, con el objeto de dañar sistemas ajenos u obtener algún tipo de rédito de sus acciones. Por lo general, el Cracker se distingue del hacker por sus valores morales.

Otro término que a menudo se relaciona con Hackers y Crackers, es el de Script Kiddies, término utilizado para referirse a aquellos hackers quienes no poseen la habilidad necesaria para llevar a cabo un ataque específico, sin para ello hacer uso de las herramientas (mayormente automáticas) que descargan de Internet o les son provistas por sus amigos. A menudo, el Script Kiddie no tiene conocimiento de cuál es exactamente la vulnerabilidad que explota, ni que es lo que hace la herramienta que utiliza.
Es de suma importancia recalcar, que el Hacking es considerado un delito en muchos países, sin importar si el hacker tuviera o no intenciones de dañar el sistema objetivo. Del mismo modo, en la literatura tradicional, suele referirse el término de Hacker, relacionado con el intruso que intenta lograr acceso no autorizado a un sistema.

2.1.6 Black Hat, Grey Hat y White Hat

En el indicador anterior, echamos un vistazo a términos como Hackers, Crackers y Script Kiddies. Adicionalmente, existe otra clasificación que a menudo es utilizada para identificar personas relacionadas con el hacking.

Black Hat, es el término con el que se llama a aquellos quienes comprometen la seguridad de un sistema, sin el permiso de su propietario, usualmente con la intención de lograr acceso no autorizado a las computadoras de la red. Por su parte, el termino White Hat, suele ser utilizado para aquellas personas quienes se encuentran éticamente opuestas al abuso de redes y sistemas.

Con frecuencia, los White Hat utilizan sus conocimientos con el objeto de proteger los sistemas de información, ya sea actuando como oficiales de seguridad, o reportando vulnerabilidades a los vendedores.

Por último Grey Hat, es el término que la comunidad utiliza para referirse a un Hacker que poseyendo la habilidad suficiente, algunas veces actúa legalmente (Tal como un White Hat) y otras no.

Estos hackers son un hibrido entre White Hat y Black Hat. Usualmente no hackean con el objetivo de obtener rédito económico, personal o causar algún tipo de daño, pero podrían o no cometer un crimen en el proceso de sus tareas o investigaciones.

2.1.7 Terminología

Los procesos involucrados en el aseguramiento de sistemas de información, son muchos y variados. Como en cualquier otra disciplina, es necesario conocer la terminología adecuada, antes de profundizar conceptos, a fin de que a posterior nos sea posible interpretar correctamente cada uno de ellos.

2.1.7.1 Activo

Cada organización tiene activos y recursos valiosos. Desde el punto de vista de la gestión de seguridad de la información, un activo puede ser un recurso, producto, proceso, dato y todo aquello que tenga un valor para la organización.

En líneas generales, a menudo los activos se encuentran divididos en dos grandes grupos:

“Tangibles” (Computadoras, servidores, dispositivos de networking, edificios, etc.) e “Intangibles” (reputación, datos, propiedad intelectual, etc.)

Un aspecto de suma importancia en todo proceso tendiente a asegurar estos activos, es el de identificación de los mismos. La identificación de activos es el proceso por medio del cual

una compañía realiza el "inventario" de todos aquellos ítems que forman parte del conjunto de recursos que se deben proteger.
Solo como un ejemplo, a continuación mencionaremos algunos de los activos que con frecuencia son asociados a sistemas de información:

• ***Recursos de información:*** bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida ("fallback"), información archivada.

• ***Recursos de software:*** software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.

• ***Activos físicos:*** equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores auto-máticos), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.

• ***Servicios:*** servicios informáticos y de comunicaciones, utilitarios generales, por ej., calefacción, iluminación, energía eléctrica, aire acondicionado.

2.1.8.2 Vulnerabilidad

Una vulnerabilidad es definida como la ausencia o debilidad de un control que puede ser explotada. Con frecuencia, solemos referirnos a una vulnerabilidad como la condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas.
Un error que habitualmente se suele cometer, es el pensar que una vulnerabilidad solo puede existir en el software, cuando en realidad el concepto es bastante más amplio, alcanzando por ejemplo la ausencia o debilidad en los controles administrativos, técnicos o físicos.

Una vulnerabilidad en el software, hardware o procedimiento, puede proveer a un atacante de la puerta de acceso que necesita para ingresar a una computadora o red de modo no autorizado, de forma tal de ganar acceso a los recursos dentro de la organización. Esta vulnerabilidad, puede ser un servicio corriendo en un servidor, un sistema operativo u aplicación sin parchear, un acceso remoto vía módem sin restricciones, un puerto abierto en un firewall, una cerradura débil o contraseñas sencillas de adivinar.

2.1.7.3 Amenaza

Es un evento cuya ocurrencia podría impactar en forma negativa en la organización. Una amenaza, es alguien o algo que habiendo identificado una vulnerabilidad específica, utiliza esta contra la compañía o el individuo.

Las amenazas, "explotan" o "toman ventaja de" las vulnerabilidades. Cuando esto sucede, solemos referirnos a la "entidad" que toma ventaja de una vulnerabilidad, como "agente de la amenaza" o por su término en inglés "threat agent". El agente de la amenaza puede ser un intruso accediendo a la red a través del puerto de un firewall, un proceso accediendo datos de manera tal que se encuentre violando la política de seguridad, un tornado arrasando con un edificio, o un empleado cometiendo un error no intencional que expone información confidencial o destruye la integridad de un archivo.

2.1.7.4 Riesgo

Es la probabilidad de que un agente de amenaza explote una vulnerabilidad, en combinación con el impacto que ocasiona, o dicho de otro modo "Riesgo" no es más que la combinación de probabilidad de ocurrencia e impacto de una amenaza.

Si un firewall tiene varios puertos abiertos, podríamos decir que existe una alta probabilidad de que un intruso utilice uno de ellos para acceder a la red por medio de métodos no autorizados. Si los usuarios no son educados acerca de procesos y procedimientos, existe una alta probabilidad de que un empleado cometa un error de modo intencional o accidental que pueda destruir datos de valor para la organización. Del mismo modo, si un IDS (Sistema de Detección de Intrusos) no es implementado sobre la red, existe una alta probabilidad de que un ataque no sea notado hasta que sea demasiado tarde.

2.1.7.5 Exposición

Es la instancia en la cual la información o un activo de información, es susceptible a dañarse o perderse por el accionar de un "agente de amenaza". La exposición, no significa que el evento que produce la pérdida o daño del recurso "este ocurriendo", solo significa que podría ocurrir dado que existe una amenaza y una vulnerabilidad que esta podría explotar.

Una vulnerabilidad, "expone" a una organización a un posible daño. Si la administración de contraseñas en una organización es débil, y no existen reglas que regulen su fortaleza, la organización podría encontrarse expuesta a la posibilidad de que las contraseñas de sus usuarios sean adivinadas o capturadas, y utilizadas de modo no autorizado. Si una organización no realiza revisiones frecuentes, respecto del estado de su cableado eléctrico, y no posee controles efectivos contra incendios en el lugar, se expone a si misma a incendios potencialmente devastadores.

2.1.7.6 Contramedida

Un proceso de suma importancia a la hora de asegurar cualquier sistema de información, es la selección de contramedidas. Formalmente, el término "Contramedida" o "Salvaguarda" es utilizado para referirnos a cualquier tipo de medida que permita detectar, prevenir o minimizar el riesgo asociado con la ocurrencia de una amenaza específica. Eventualmente las "Contramedidas" o "Salvaguardas" suelen recibir el nombre de "Controles".

Una contramedida puede ser una configuración específica en un software, un dispositivo de hardware, o un procedimiento que elimine una vulnerabilidad o reduzca la probabilidad de que el "agente de amenaza" sea capaz de explotar dicha vulnerabilidad.

Algunos ejemplos de contramedidas incluyen contraseñas fuertes, guardias de seguridad, mecanismos de control de acceso dentro del sistema operativo, la implementación de contraseñas a nivel de BIOS, concientización del personal, etc.

2.1.8 Relación entre los conceptos

Todos los conceptos se encuentran relacionados entre sí de diferentes formas. Para un mejor entendimiento proporcionamos los siguientes ejemplos: Si una compañía posee un software antivirus pero este no tiene sus firmas actualizadas, esto es una vulnerabilidad. La

compañía es vulnerable al ataque de un virus. La amenaza es que el virus se distribuya dentro de la organización, aparejando pérdida de productividad, mientras que el riesgo no es otro que el que el virus disperso por toda la organización cause daño.

Si un virus se infiltra en la compañía, entonces una vulnerabilidad ha sido explotada y la compañía se encuentra expuesta a perdidas. Por su parte, la contramedida en este caso es la de actualizar las firmas e instalar el software en todas y cada una de las computadoras que forman parte de la red de la compañía.

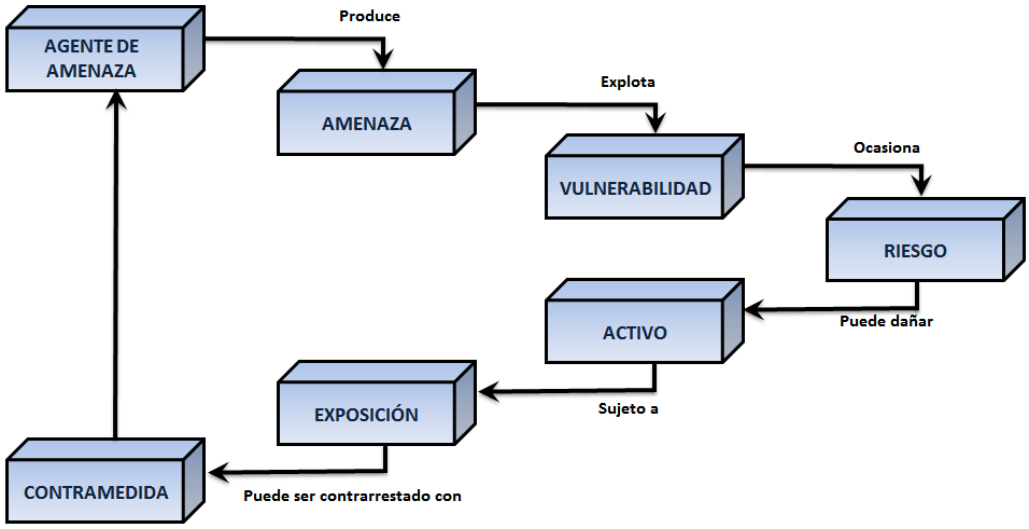


Figura 2.3 Relación entre Conceptos

2.2 Ataque Informático

2.2.1. Definición

"Método por el cual, valiéndose de una vulnerabilidad y sin tener el permiso correspondiente, o sin validarse o identificarse, se puede realizar una negación de servicio, ejecutar código arbitrario, obtener información confidencial, escalar privilegios, administrar el sistema, tomar el control del mismo, o simplemente detener o dañar el sistema informático" [WEB 01]

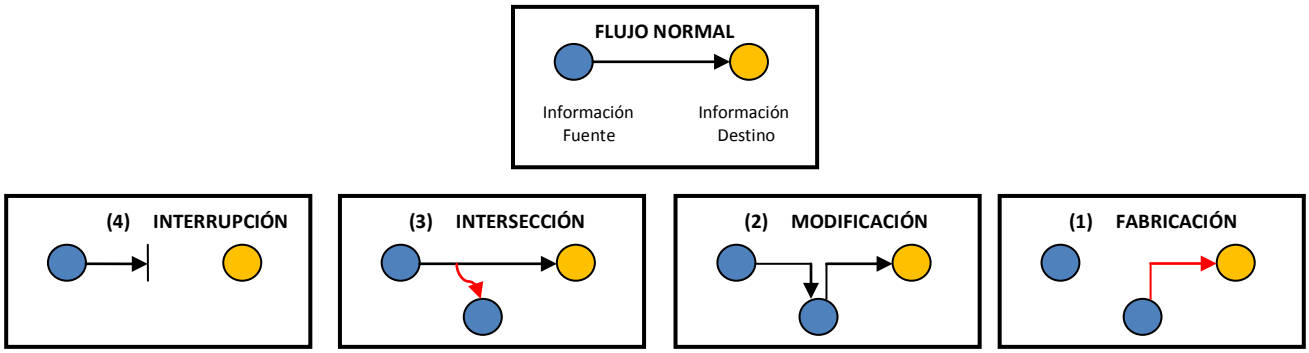
2.2.2. Modelo de proceso de ataque informático

El modelo se concentró básicamente en la información en tránsito. Se define cuatro categorías de ataque:

- **Interrupción**: Se realiza cuando en el tránsito de la información se interrumpe el activo, donde se podría destruir o poner no disponible.
- **Intersección**: Una aparte no autorizada gana acceso a un activo
- **Modificación**: Una parte no autorizada no solo gana acceso a un activo, sino que lo manipula el activo.
- **Fabricación**: Una parte no autorizada inserta un objeto falsificado en el sistema.

Según el autor lo clasifica como ataque pasivo a la intersección y cómo ataque activo a la interrupción, modificación y fabricación. [STA95]

Figura 2.4 Modelo de proceso de ataque informático



2.2.3. Principales ataques informáticos

2.2.3.1 Ingeniera Social

Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y Contraseña. Los ingenieros sociales manipulan y explotan los sentimientos y emociones de los usuarios legítimos tales como el miedo, la curiosidad, el sexo, la avaricia, la compasión y el deseo de agradar y de hacer bien su trabajo, con el objetivo de obtener información confidencial.

La principal defensa contra la ingeniería social es educar y entrenar a los usuarios en el uso de políticas de seguridad y asegurarse de que estas sean seguidas. Uno de los ingenieros sociales más famosos de los últimos tiempos es Kevin Mitnick. [WEB02]

2.2.3.1.1 Phishing

Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

2.2.3.2 Trashing

Técnica que se utiliza muy poco, que consiste en buscar información en los cubos de basura de las empresas, tales como: información sobre los sistemas, reportes, documentos, datos de usuarios, disquetes aparentemente dañados. Por ejemplo un usuario anota su usuario y contraseña en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema.

2.2.3.3. Shoulder Surfing

Consiste en espiar físicamente a los usuarios para obtener el usuario y su contraseña correspondiente. El Surfing explota el error de los usuarios de dejar su usuario y contraseña anotados cerca de la computadora (generalmente en post–it adheridos al monitor o teclado). Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso. Otra técnica relacionada al surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y contraseña.

2.2.3.4 Scanning

El Scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoría también se basan en este paradigma.

Scanear puertos implica las mismas técnicas de fuerza bruta. Se envía una serie de paquetes para varios protocolos y se deduce que servicios están "escuchando" por las respuestas recibidas o no recibidas. Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

2.2.3.4.1 TCP Connect Scanning

Esta es la forma básica del scaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con él.

Las ventajas que caracterizan esta técnica es que no necesita de privilegios especiales y su gran velocidad y su principal desventaja es que este método es fácilmente detectable por el administrador del sistema. Se verá un gran número de conexiones y mensajes de error para los servicios en los que se ha conseguido conectar la máquina, que lanza el scanner, y también se verá su inmediata desconexión.

2.2.3.4.2 TCP SYN Scanning

El establecimiento de conexión entre el servidor y el cliente se realiza mediante lo que se llama Three-Way Handshake ("conexión en tres pasos") ya que intercambian tres segmentos.

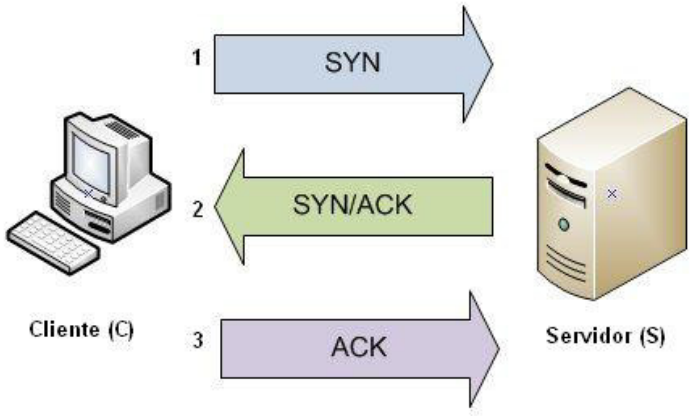
Proceso:

1. El programa Cliente (C) pide conexión al Servidor (S) enviándole un segmento SYN. Este segmento le dice a S que C desea establecer una conexión.
2. S (si está abierto y escuchando) al recibir este segmento SYN (activa el indicador) y envía una autentificación ACK de manera de acuse de recibo a C. Si S está cerrado envía un indicador RST.

3. C entonces ACK (autentifica) a S. Ahora ya puede tener lugar la transferencia de datos.

   En forma esquemática se tiene:

Figura 2.5 Establecimiento de la conexión TCP



Cuando las aplicaciones conectadas terminan la transferencia, realizaran otra negociación a tres bandas con segmentos FIN en vez SYN.

La técnica, implementa un scaneo de "media-apertura", dado que nunca se abre una sesión TCP completa. Se envía un paquete SYN (como si se fuera a usar una conexión real) y se espera por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.

La principal ventaja de esta técnica de escaneo es que pocos sitios están preparados para registrarlos. La desventaja es que en algunos sistemas Unix, se necesitan privilegios de administrador para construir estos paquetes SYN.

2.2.3.4.3 TCP FIN Scanning

Hay veces en que incluso el scaneo SYN no es lo suficientemente "clandestino" o limpio. Algunos sistemas (Firewalls y filtros de paquetes) monitorizan la red en busca de paquetes SYN a puertos restringidos.

Para subsanar este inconveniente los paquetes FIN, en cambio, podrían ser capaces de pasar sin ser advertidos. Este tipo de Scaneo está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión.

2.2.3.4.4 Fragmentation Scanning

Esta no es una nueva técnica de scaneo como tal, sino una modificación de las anteriores. En lugar de enviar paquetes completos de sondeo, los mismos se particionan en un par de pequeños fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudieran estar ejecutándose en la máquina objetivo.

Sin embargo, algunas implementaciones de estas técnicas tienen problemas con la gestión de este tipo de paquetes tan pequeños, causando una caída de rendimiento en el sistema del intruso o en el de la víctima. Problemas de esta índole convierte en detectables a este tipo de ataque.

2.2.3.5 Sniffing

Esta técnica utiliza programas que monitorean los paquetes que circulan por la red. Los Sniffers pueden ser colocados tanto en una estación de trabajo conectada a la red, como a un equipo Router o a un Gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías.

El programa se configura un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a computadora donde está instalado el Sniffer.

Actualmente existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo passwords de un recurso compartido o de acceso a una cuenta, que generalmente viajan sin cifrar al ingresar a sistemas de acceso remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes.

2.2.3.6 Snooping

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla. Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, para luego hacer un análisis exhaustivo de la misma.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron: el robo de un archivo con más de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

2.2.3.7 Spoofing

El objetivo de esta técnica, es engañar al sistema de víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y contraseña.

El envío de falsos e-mails es otra forma de Spoofing que las redes permiten. Aquí el atacante envía e-mails a nombre de otra persona con cualquier motivo y objetivo. Tal fue el caso de una universidad en EE.UU. que en 1998, que debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina de estudiantes. [WEB03]

2.2.3.7.1 Spoofing Sobre Protocolos

Este tipo de ataques suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son:

2.2.3.7.1.1 IP Spoofing

Suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente

gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UDP o TCP. Este ataque se hizo famoso al usarlo Kevin Mitnick.

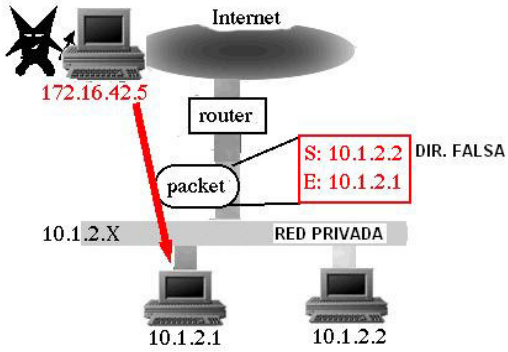


Figura 2.6 Ataque IP Spoofing

2.2.3.7.1.2 DNS Spoofing

Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Esto se consigue falseando las entradas de la relación Nombre de dominio-IP de un servidor DNS, mediante alguna vulnerabilidad del servidor en concreto o por su confianza hacia servidores poco fiables.

Escenario: La compañía, TAMJTeK Inc., está compitiendo para acabar el desarrollo del último software de juegos. Se comienza a anunciar el aviso de este juego en el sitio Web de Internet. Usted tiene una llamada de uno de los socios de la empresa. Ella desea saber por qué termina llegando a www.hackncrack.net cuando intenta llegar a www.tamjtek.com.

Usted intenta conectarse al sitio Web y, seguro, termina llegando a www.hackncrac.net. Usted prueba algunos otros sitios y todo parece muy bien excepto, que encuentra que su competidor más fuerte ha anunciado el mismo juego. Su sitio Web demuestra una imagen de su juego, la cual parece notablemente similar a la suya con aspectos virtualmente idénticos. ¿Coincidencia? Quizás no. [WEB 04]

2.2.3.7.1.3 Web Spoofing

Suplantación de una página web real. Enruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información de dicha víctima

2.2.3.7.1.4 Mail Spoofing

Suplantación en correo electrónico de la dirección e-mail de otras personas o entidades con contenido falso o engañoso y atrayente. Normalmente es distribuido en cadena por sus sucesivos receptores debido a su contenido impactante que parece provenir de una fuente seria y fiable.

2.2.3.8 Hijacking

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima se identifique ante el sistema y tras ello le suplanta como usuario autorizado. Las variaciones son las siguientes: IP hijakers, Page hijacking, Domain hijacking, Session hijacking, Browser hijacking y Home Page Browser hijacking.

2.2.3.9 Utilización De Backdoors

"Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas.
Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo" [HUE02].
Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.

2.2.3.10 Utilización de Exploits

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o implemente encontrando un error en los programas utilizados.

Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo.

2.2.3.11 Obtención de Contraseñas

La obtención de la contraseña que permiten ingresar a los sistemas, se puede realizar por el método de "Fuerza Bruta": Este ataque consiste en la técnica de prueba y error, ya que muchas contraseñas se consiguen fácilmente ya que involucran nombres o datos de familiares del usuario y que muy rara vez lo cambian. También se e realizan ataques sistemáticos con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la contraseña correcta.

2.2.3.12 Negación de Servicio (DOS)

La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Listaré las razones importantes por las cuales este tipo de ataques pueden ser útiles:

1. Se ha instalado un troyano y se necesita que la víctima reinicie la máquina para que surta efecto.
2. Se necesita cubrir inmediatamente sus acciones o un uso abusivo de CPU. Para ello provoca un "crash" del sistema, generando así la sensación de que ha sido algo pasajero y raro.
3. El intruso cree que actúa bien al dejar fuera de servicio algún sitio web que le disgusta. Este accionar es común en sitios pornográficos, religiosos o de abuso de menores.
4. El administrador del sistema quiere comprobar que sus instalaciones no son vulnerables a este tipo de ataques.
5. El administrador del sistema tiene un proceso que no puede "matar" en su servidor y, debido a este, no puede acceder al sistema. Para ello, lanza contra sí mismo un ataque DoS deteniendo los servicios.

- **Flooding**

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando Spoofing . El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos Hosts de Internet han sido dados de baja por el "ping de la muerte" Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el bloqueo instantáneo del equipo. Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los sistemas destinos.

- **Syn Flood**

Como ya se explicó en el TCP SYN Scanning el protocolo TCP se basa en una conexión en tres pasos. Pero, si el paso final no llega a establecerse, la conexión permanece en un estado denominado "semiabierto".

El Cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el Host hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna), el Servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios. SYN Flood aprovecha la mala implementación del protocolo TCP.

- **Connection Flood**

La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultáneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo,

capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del SYN Flood) para mantener fuera de servicio el servidor.

- **Net Flood**

El ataque consiste en saturar a la red de tráfico malicioso, incapacitándolas para cursar tráfico útil. El atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir. Si el atacante emplea IP Spoofing, el rastreo puede ser casi imposible, ya que en muchos casos la fuente del ataque es, a su vez, víctima y el origen último puede ser prácticamente imposible de determinar (Looping).

- **Smurf**

Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones BroadCast para, a continuación, mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen (máquina víctima).

Este paquete maliciosamente manipulado, será repetido en difusión (Broadcast), y cientos ó miles de hosts mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP.

- **Winnuke**

Se refiere a un ataque informático de denegación de servicio que afectaba al sistema operativo Microsoft Windows 95.

Consistía en enviar una determinada cadena al puerto 139 de TCP (NetBIOS) que bloqueaba al sistema operativo hasta que aparece la pantalla azul.

2.2.3.13 Replay

También denominado "ataques de reinyección", es una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado. El ataque de replay pretende capturar información y posteriormente reenviarla con el objetivo de falsificar la identidad de uno de los lados.

2.2.3.14 Man-in-the-middle

También conocido como "**MitM"** o *intermediario*, en castellano, es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

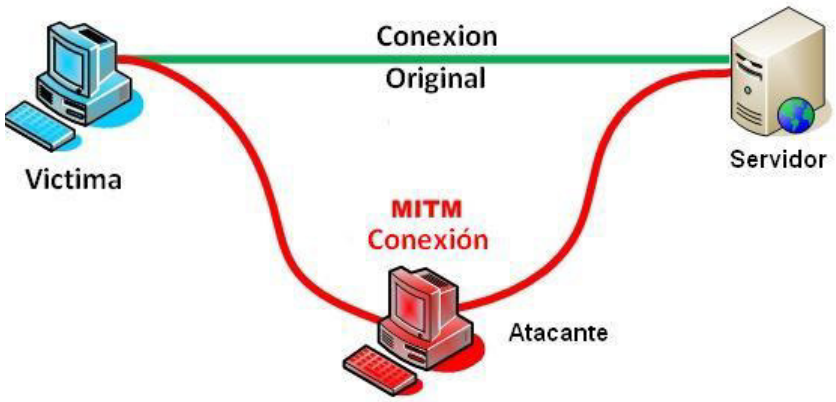


Figura 2.7 Ataque Hombre en el medio

2.3. Virus Informáticos

2.3.1 Definición

Pequeños programas en lenguajes de programación que son desarrollados para causar daños a los sistemas, contienen rutinas de propagación, susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o destrucción de los programas, información y/o hardware afectados (en forma lógica) [BOR09].

2.3.2 Técnicas de Propagación

Actualmente las técnicas utilizadas por los virus para logra su propagación y subsistencia son muy variadas y existen aquellos que utilizan varias de ellas para lograrlo.

1. Disquetes y otros medios removibles
2. Correo electrónico
3. IRC o Chat.
4. Páginas web y transferencia de archivos vía FTP:
5. Grupos de noticias:

2.3.3 Tipos de los Virus

2.3.3.1 Virus De Boot que infectan la memoria y atacan al sector de arranque de los diskettes y el disco duro y desde cuya posición pueden infectar a los archivos y áreas del sistema que su creador haya decidido afectar.

2.3.3.2 Virus de Archivos Ejecutables

Los virus infectan archivos del sistema operativo para ser ejecutados. Una vez activados atacarán a otros archivos ejecutables o áreas, haciendo copias de sí mismos, sobrescribiéndolos o alterando archivos de cualquier otra extensión, no ejecutables.

2.3.3.3 Macrovirus

Afecta documentos de Microsoft Word, utilizando las funcionalidades de las macros para llevar a cabo sus acciones. No suelen provocar grandes daños, pero sí son molestos.

Su funcionamiento consiste en que si una aplicación abre un archivo infectado, la aplicación (o parte de ella) se infecta y cada vez que se genera un nuevo archivo o se modifique uno existente contendrá el macrovirus.

2.3.3.4 Virus de Mail

El usuario recibe un mensaje vía mail con un archivo comprimido (.ZIP por ejemplo), el usuario lo descomprime y al terminar esta acción, el contenido (virus ejecutable) del archivo se ejecuta y comienza el daño. Ejemplo el virus Melissa y I Love You. Generalmente estos virus se auto envían a algunas de las direcciones de la libreta. Cada vez

que uno de estos usuarios recibe el supuesto mensaje no sospecha y lo abre, ocurriendo el mismo reenvío y la posterior saturación de los servidores al existir millones de mensajes enviados.

2.3.3.5 Virus Fantasmas

El auge del correo electrónico generó la posibilidad de transmitir mensajes de alerta de seguridad. Así comenzaron a circular mensajes de distinta índole (virus, cadenas solidarias, beneficios, catástrofes, etc.) de casos inexistentes. Los objetivos de estas alertas pueden causar alarma, la pérdida de tiempo, el robo de direcciones de correo y la saturación de los servidores con las consecuentes pérdidas de dinero que esto ocasiona.

2.3.3.6 Gusanos

Programa de software que es diseñado para copiarse a sí mismo de una computadora a otra, sin interacción humana. A diferencia de los virus computacionales, un gusano puede copiarse automáticamente. Los gusanos se pueden replicar en gran volumen. Por ejemplo, un gusano puede enviar copias de sí mismo a cada contacto de correo electrónico en su libreta de direcciones y podría de ahí enviarse a todos los contactos de esas libretas de direcciones

2.3.3.7 Caballos de Troya

Un troyano es similar a un virus, es un programa que busca propagarse y sobre todo a través de aplicaciones de Internet como el EMAIL, ICQ y CHAT. La diferencia básica de los troyanos con los virus es que los troyanos están hechos para permitirles a otras personas tener acceso al contenido de la PC infectada ya sea para robar información, contraseñas, documentos, datos, etc. Son muy peligrosos, porque pueden capturar y reenviar datos confidenciales a una dirección externa, abrir puertos de comunicaciones para que un intruso pueda entrar y salir de nuestro sistema las veces que se le antoje.

2.3.3.8 Bombas Lógicas

Este suele ser el procedimiento de sabotaje más comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada o

dado algún evento particular en el sistema, bien destruye y modifica la información o provoca la baja del sistema.

2.3.4 Modelo de Virus Informático

Un virus está compuesto por su propio entorno, dentro del cual pueden distinguirse tres módulos principales:

- **Módulo de Reproducción**

  Es el encargado de manejar las rutinas de parasitación de entidades ejecutables con el fin de que el virus pueda ejecutarse a escondidas, permitiendo su transferencia a otras computadoras.

- **Módulo de Ataque**

  Es el que maneja las rutinas de daño adicional al virus. Esta rutina puede existir o no y generalmente se activa cuando el sistema cumple alguna condición. Por ejemplo el virus Chernovil se activa cada vez que el reloj del sistema alcanza el 26 de cada mes.

- **Módulo de Defensa**

  Este módulo, también optativo, tiene la misión de proteger al virus. Sus rutinas tienden a evitar acciones que faciliten o provoquen la detección o remoción del virus.

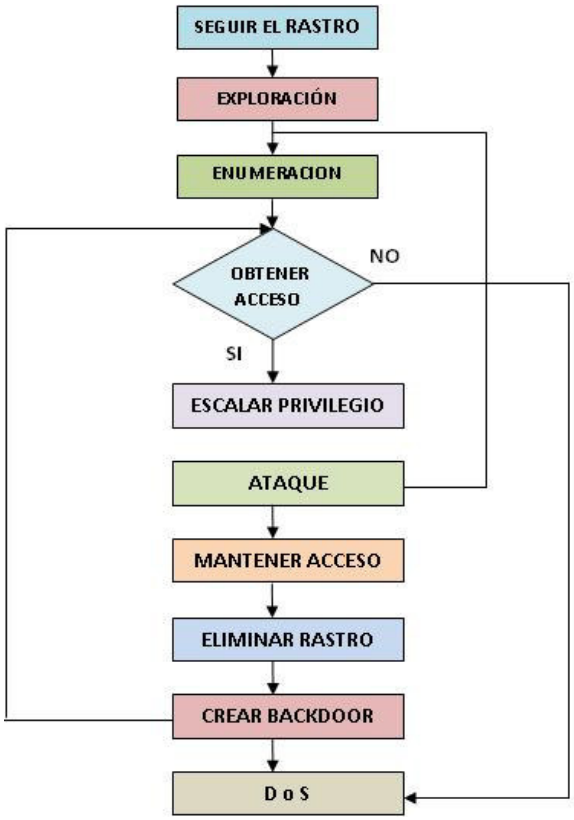
2.3.5 Fases del ataque informático

En el siguiente punto detallamos las 10 fases del ataque:

1. Seguimiento del rastro
2. Exploración
3. Enumeración
4. Obtener Acceso
5. Escalar Privilegios
6. Ataque
7. Mantener el acceso
8. Eliminando Rastros

9. Colocación de puerta trasera
10. Negación de Servicio

Figura 2.8 Fases de la anatomía de un ataque



2.3.5.1 Seguir el Rastro

Esta es la primera fase del ataque, en el cual se define el objetivo a atacar, sea una red, un servidor remoto, una página web, una aplicación cliente/servidor, hardware, una compañía, etc. En este punto el atacante intentará reunir, localizar, obtener y guardar tanta información del objetivo como le sea posible, mediante el método de la Ingeniería Social.

Las técnicas de reconocimiento de forma general se clasifican en 2, activas y pasivas.

a. Pasivas: El atacante utiliza información pública (sitio web de la empresa), Ingeniería Social y algunos otros métodos. En esta forma no se interacciona de forma directa con el sistema.

b. Activas: El atacante interacciona de forma directa con el sistema buscando puertos abiertos, creando un mapa de la red, equipos accesibles y detalle de los sistemas operativos utilizados.

2.3.5.2 Exploración

Se realiza algún tipo de conexión ya sea desde la máquina del atacante, algún servidor *proxy* o alguna máquina comprometida. De forma general se usan herramientas automáticas como un escáner de red, host, marcadores masivos, etc. El atacante buscará extraer información como el software utilizado, versiones del sistema operativo, la infraestructura en la red, routers y cortafuegos. Algunas de estas actividades pueden ser realizadas con herramientas tan simples como traceroute.

En la fase de exploración se utilizan la técnica de footprinting que utiliza herramientas como Ping, Fping, P0f, Nmap, Hping, Xprobe, etc.

Pasos para realizar el Footprinting son los siguientes:

1. Información inicial
2. Localizar rangos IP
3. Comprobar maquinas activas
4. Descubrir puertos abiertos o puntos de acceso
5. Detectar los sistema operativos
6. Descubrir los servicios en los puertos abiertos
7. Hacer el mapa de red.

2.3.5.3 Enumeración

El objetivo es identificar las cuentas de usuarios administrativos y normales del sistema para luego obtener escalada de privilegios en caso de tomar un usuario normal, existe una herramienta muy útil llamada DumpSec, que permite la enumeración de usuarios, grupos, permisos, también la herramienta Hyena logra esta enumeración muy rápido en un entorno de dominio o grupo de trabajo.

2.3.5.4 Obtener Acceso

El atacante que ha obtenido acceso, con la técnica del crackeo de contraseña u otra herramienta. También en ocasiones el ataque no necesariamente depende de obtener el acceso, puede ser que se realice alguna denegación de servicio.

Obtener el acceso es uno de los pasos más importantes en el proceso del ataque, significa el cambio de realizar pruebas en la red (exploración y enumeración) a penetrar en la red, el acceso puede ser a nivel de sistema, aplicación o de red.

2.3.5.5 Escalar Privilegios

El proceso de escalar privilegios se puede definir como la explotación de alguna vulnerabilidad en la aplicación o sistema operativo que permita sobrepasar las restricciones impuestas para los usuarios promedio, lo que da como resultado un acceso completo al sistema.

En esta etapa ya se tiene un usuario valido en el sistema, el cual puede tener permisos mínimos por esta razón se debe añadir más permisos o derechos a la cuenta de usuario que se tiene, la idea es volverlo administrador del sistema para instalar y ejecutar aplicaciones, para realizar esto existe un troyano llamado GetAdmin.exe, lo cual realiza esto en los sistemas Windows NT, pero es detectable por la mayoría de Antivirus.

2.3.5.6 Ataque

Esta es la parte más emocionante de un hacker, realizar el ataque del sistema, ya que su ego y su capacidad de lograrlo es lo que lo motiva mas para realizar ataques más sofisticados, He aquí la fórmula secreta de un ataque:

ATAQUE = Amenazas + Motivos + Herramientas y técnicas + Puntos Vulnerables

A nivel de ataques tenemos la Denegación de Servicio (DoS), Session Hijacking o secuestro de sesión, Spoofing o el uso de técnicas de suplantación de identidad como IPs, ARPs, DNS, WEB, correo electrónico. Ataques a Nivel de Aplicaciones, lo más común es

encontrar las vulnerabilidades a nivel de sistema operativo, como las configuraciones por defecto, el código de programación, instalación por defecto, falta de actualización de parches de seguridad y falta de políticas de seguridad adecuadas.

2.3.5.7 Mantener el acceso

En esta fase el intruso intenta permanecer en el sistema, el cual ha comprometido. Algunas de las actividades que realizará son agregar usuarios con altos privilegios, robar contraseñas de otros usuarios o servicios (mediante *sniffers*, *keyloggers*) incluso en algunas ocasiones instalará herramientas como *rootkits*, *troyanos*. Un *rootkit* es un conjunto de herramientas que le permite al atacante ocultar sus actividades (procesos, sesiones, conexiones) pueden ser a nivel aplicación o incluso a nivel de núcleo.

2.3.5.8 Eliminando Rastros

Esta fase se refiere a todas las acciones que realizará el atacante para cubrir su rastro y poder incrementar el mal uso del sistema sin ser detectado.

Normalmente el atacante elimina la evidencia del ataque y de sus actividades (instalación de programas, *rootkits*) para evitar acciones legales, andar libremente en el sistema comprometido, mantener el acceso, etc.

Las técnicas más comunes son: eliminar la evidencia de los archivos de registro (*logs*). El atacante debe ser cuidadoso con los archivos o programas que deja en el sistema comprometido. Usará técnicas para ocultar archivos, directorios, atributos ocultos.

2.3.5.9 Creación de puerta trasera

Las puertas traseras son un método utilizado para regresar al sistema sin volverlo a explotar. Algunas otras técnicas son la esteganografía y la utilización de túneles en TCP.

Aquí puede comenzar de nuevo el ciclo del ataque, pero ahora realizando el reconocimiento sobre otro objetivo.

Cabe destacar que en algunos casos, teniendo una máquina comprometida, el ataque hacia otro objetivo puede resultar mucho más sencillo. Esto se debe a que el atacante podría no preocuparse ya de ser tan precavido.

2.3.5.10 Negación de Servicio

Si el atacante no logra obtener acceso, un recurso que puede llevar a cabo es la denegación de servicio. Esto es a causa de que no tenga los conocimientos suficientes para llevar a cabo la penetración o por el simple hecho de decir "Si yo no tengo acceso, entonces que nadie tenga".

La denegación de servicio es un ataque devastador, su objetivo principal es denegarles a los usuarios legítimos el acceso a los recursos necesarios.

2.4 Tecnología UTM

UTM es un término acuñado originalmente por **IDC,** compañía de investigación de mercado.

Según IDC: "UTM dispositivos de seguridad, incluyen múltiples características de seguridad en una caja. Para ser incluido en esta categoría, a diferencia de otros segmentos, el aparato debe contener la posibilidad de realizar firewalling de red, detección de intrusos de red y la prevención, y antivirus gateway. Todas las capacidades en el aparato no tiene que ser utilizado, pero las funciones deben existir intrínsecamente en el aparato. En estos productos, los componentes individuales no pueden ser separados"

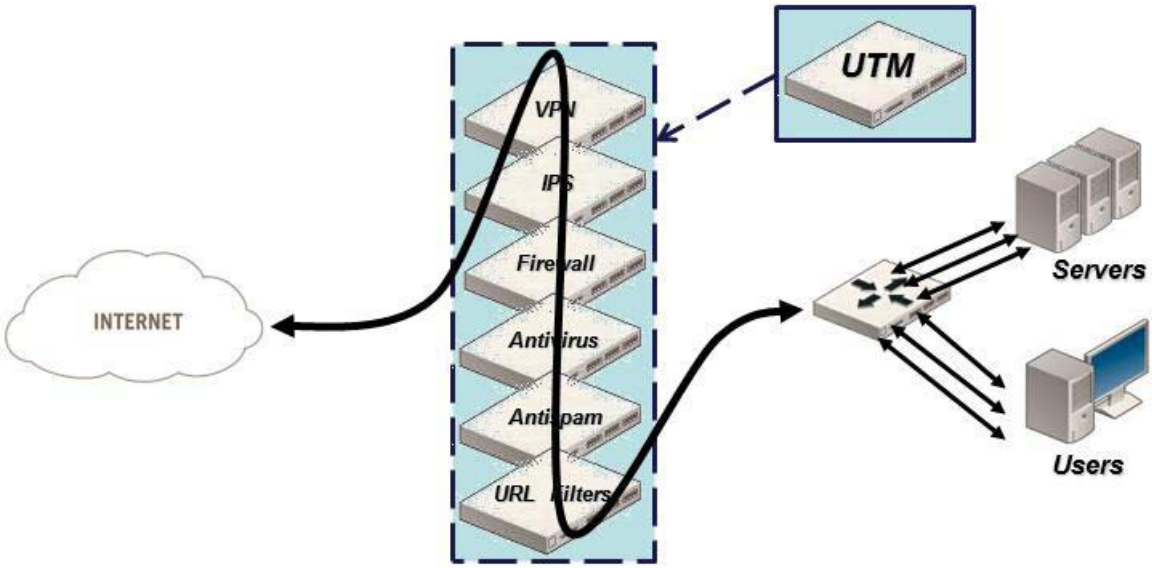


Figura 2.9 Enfoque tradicional de Seguridad

Corresponden a la tendencia más seguida en la actualidad y ampliamente difundida en las empresas. Consolidan gran cantidad de servicios de seguridad en una sola máquina, como VPN, IDS, IPS, Mail Gateway, Antivirus, Antispam, Web Proxy, NAT, DHCP Server, entre muchos otros.

Tradicionalmente, las mejores prácticas y administración del sistema de seguridad dicen que es bueno y recomendable tener uno o varios dispositivos para realizar una sola función. De esta manera, si un dispositivo falla, sólo un servicio se vería afectado, cuestión que puede ser mitigado por al menos dos dispositivos que realiza la misma función en una configuración de alta disponibilidad. Esto no presenta en las grandes empresas que cuentan con los recursos suficientes y dispone del personal para administrar estos equipos. Pero en las pequeñas y medianas empresas debido a la falta de personal y limitaciones presupuestarias estos equipos que realizan varias funciones a la vez resultan útiles y son muy necesarios.

"La Gestión Unificada de Amenazas (UTM)" es una solución completa que ha surgido recientemente en la seguridad de las redes de la industria y, desde 2004, ha ganado aceptación general como una solución de protección.

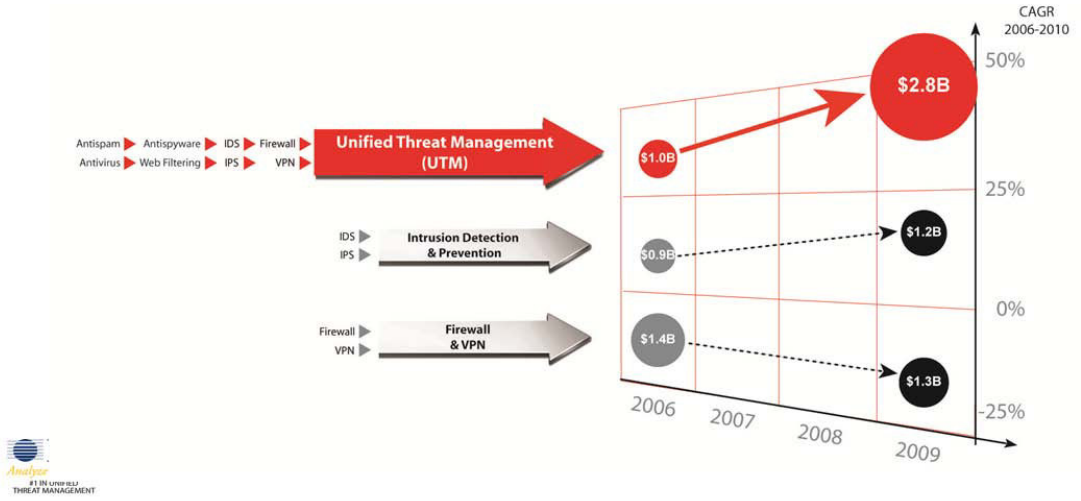


Figura 3.0 Aceptación de equipos UTM en el mercado

El mercado mundial de UTM aproximadamente alcanzó 1,2 millones en 2007, con una previsión del 35-40% tasa compuesta de crecimiento anual hasta el 2011. Algunos de los proveedores líderes que proporcionan appliances de seguridad con tecnología UTM son: Astaro, Check Point , Fortinet , Juniper , SonicWall , Wiresoft, Watchguard .
Recientemente, la UTM ha anunciado su caída de la tasa de crecimiento de 20,1% en 2009 frente al 32,2% en 2008, debido a la recesión, según un nuevo análisis.

2.4.1 Antecedentes

UTM surgió de la necesidad de detener el creciente número de ataques contra los sistemas de información corporativa a través de:

• **Acceso generalizado a Internet:** el acceso a Internet desde diferentes dispositivos ha convertido a cada casa, oficina o partner de negocios en un potencial punto de entrada de los ataques. Este acceso generalizado expone a la red empresarial a ataques sofisticados que pueden ser lanzados por algún hacker o por un usuario remoto que al "logearse" a la red corporativa permita un ataque de tipo "piggy-back". La moda de trabajar en casa y de usar la PC del trabajo para usos personales aumenta la posibilidad de ataques como Spyware, Phishing o SPAM, por lo que este problema debe ser tratado al nivel de la red corporativa. Un estudio realizado en 2005 por CSI FBI dio a conocer que el 65 por ciento de las empresas auditadas sufrieron algún ataque de una fuente externa.

• **Ataques internos**: mientras que frenar los ataques externos representa un desafío constante, igualmente de difícil y engorroso resulta defenderse de los ataques perpetuados desde adentro de la red por empleados que tienen acceso y control total de los recursos de la red. Los ataques internos van desde el acceso a los recursos hasta la destrucción o robo de información delicada.

• **Cambiando los niveles de acceso:** Una gama cada vez más extensa de acceso a la red se concede a empleados y no empleados, volviendo más vulnerable la red. Los empleados remotos, partners de negocios, clientes y proveedores pueden tener diferentes niveles de acceso a los recursos de la empresa, por lo que se deben tomar las medidas adecuadas para

proteger la red empresarial. Mientras que aumentan las aplicaciones a las que los usuarios remotos tienen acceso a través del DMZ, las compañías tratan de reducir los costos minimizando las aplicaciones entre usuarios internos y externos, lo que hace necesario acomodar las aplicaciones usadas por ambos grupos.

El mercado primario de los proveedores de UTM es el SMB y el segmento de empresa, aunque algunos proveedores están ofreciendo soluciones UTM para pequeñas oficinas / oficinas remotas.

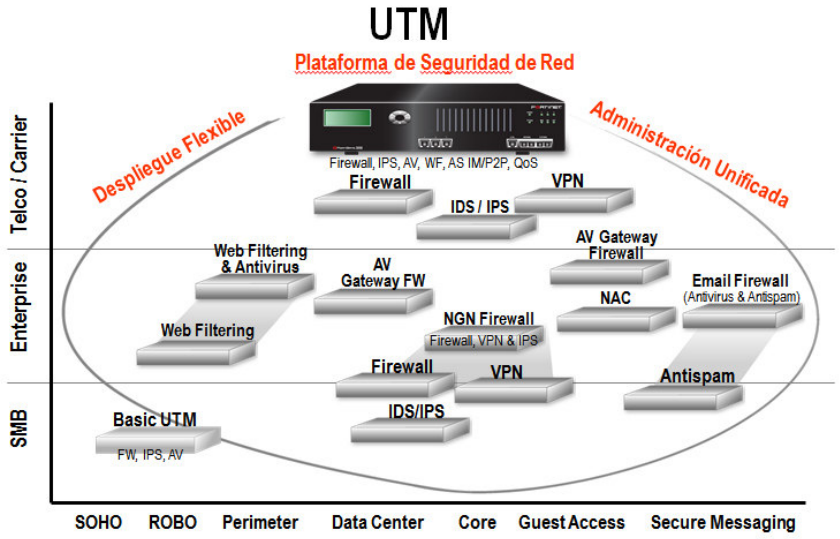


Figura 3.1 Plataforma UTM

2.4.2 Funcionamiento

Los analistas de industrias y los expertos en seguridad coinciden en que la clave para encontrar un balance entre la seguridad de la red restrictiva y el acceso que necesitan los empleados, partners de negocios y clientes se necesita la implantación de dispositivos UTM. [WEB 05]

Un dispositivo UTM único hace que sea muy fácil gestionar la gestión de seguridad de una empresa al abarcar diversas funcionalidades de protección en un mismo dispositivo.

Desde una única consola centralizada, todas las soluciones de seguridad pueden ser controladas y configuradas.

La UTM puede ser muy eficaz, porque su fuerza radica en el paquete de soluciones que se integran y diseñados para trabajar juntos.

Esta solución le da al departamento de IT un completo conjunto de herramientas que se pueden utilizar para alcanzar la seguridad end-to-end desde el sitio remoto hasta el data center. La solución está diseñada para proteger los recursos críticos de la red. Si falla una capa, la siguiente detendrá el ataque o disminuirá el daño que pueda provocar.

COMPONENTE	DESCRIPCIÓN
Red Privada Virtual – VPN	Protege las comunicaciones entre los sitios y/o los usuarios con una sesión cifrada y autenticada.
Firewall	Protege la red mediante el control de quién y qué tipo de acceso de red tiene cada persona. Detiene el tipo de ataque (DoS).
IDS/IPS	Combinación de protección que detecta y frena los ataques a nivel de las aplicaciones
Antivirus	Protección contra los ataques de virus.
Filtro de Contenido	Frena a los usuarios de visitar páginas web inapropiadas o bajar spyware u otra aplicación maliciosa desde sitios desconocidos
AntiSpam	Reduce la cantidad de correo no deseado

Tabla 2.1 Componentes del Dispositivo UTM

El objetivo final de una UTM es proporcionar un conjunto completo de características de seguridad en un solo producto y gestionado a través de una única consola. Las soluciones integradas de seguridad se desarrollaron como una forma lógica de abordar la compleja mezcla de amenazas en Internet que cada vez causaban más impacto en las organizaciones.

La UTM puede ser muy eficaz, porque su fuerza radica en el paquete de soluciones que se integran y diseñados para trabajar juntos.

2.4.3 Componentes del Dispositivo UTM

Es un hecho aceptado que las intrusiones y los ataques son inevitables y que las estrategias de seguridad por capas compuestas de múltiples tecnologías complementarias de seguridad, todas trabajando en forma conjunta, ayudan a minimizar el riesgo al interponer múltiples barreras entre el atacante y su objetivo.

Esta estrategia también le da al administrador de redes más tiempo para reaccionar y evitar mayores daños una vez que el ataque ya ocurrió.

2.4.3.1 Firewall: control de acceso y autenticación

El firewall actúa como la primera capa de la seguridad controlando quién o qué tiene acceso a la red. El firewall realiza una inspección de estado (stateful inspection) para proteger a la red del contenido malicioso. Con esta inspección se recoge información de las sesiones TCP y UDP como la dirección IP de la fuente y del destinatario, el número de puerto de la fuente y del destinatario y los números de secuencia del paquete y se mantiene esta información para analizar el tráfico en un futuro.

2.4.3.2 IDS/ IPS

La solución de Detección de Intrusos permite identificar solamente los ataques y generar alarmas, pero no puede bloquear el ataque. La solución de Prevención de Intrusos permite detectar y bloquear los ataques ocurridos en el perímetro de la red, evitando que el ataque alcance a los servicios en los servidores. Además, de controlar y restringir a los usuarios o grupos en el uso del P2P y Mensajería Instantánea causante muchas veces de fuga de información y entrada de virus, spyware y ataques.

2.4.3.3 Virtual Private Networks – VPN

La siguiente capa de protección utiliza una Virtual Private Network (VPN) para cifrar las comunicaciones que atraviesan un medio poco confiable como Internet o un segmento interno de la red. Existen dos tipos de soluciones VPN: IPSec VPN o SSL VPN. Una IPSec VPN asume que los dos endpoints, site-to-site o client-to-site, están conectados a través de una conexión de red virtual.

Con una IPSec VPN, los usuarios teóricamente tienen acceso a todos los recursos de la red. Una SSL VPN establece una conexión encriptada desde un browser hacia la aplicación deseada o conjunto de aplicaciones basadas en la credencial de un usuario. Este método de acceso permite que el usuario se "loguee" en el sistema pero con un control de qué aplicaciones están disponibles teniendo en cuenta el nivel de confianza del end point.

- **Site-to-Site VPN**

  Esta solución de VPN supone una comunicación de dispositivo a dispositivo con toda la información entre ellos protegida mediante la encriptación y un túnel autenticado. Con una VPN site-to-site, todos los usuarios mantienen una comunicación segura con el destino, la cual es más segura utilizando IPSec VPN.

- **Remote Access VPN**

  Esta solución VPN es típicamente implementada para los usuarios remotos como los teleworkers, partners de negocios, proveedores y otros usuarios remotos que requieran de acceso a los recursos de la red. Dependiendo de lo que se necesite, IPSec o SSL VPN pueden brindar un acceso remoto VPN. Como SSL VPN no necesita implementación, instalación o configuración de software en la máquina del usuario, es una atractiva solución para los empleados y los clientes. SSL VPNS son, además, particularmente efectivas a la hora de conectar a los recursos internos de la empresa con los partners de negocios o con los clientes donde la instalación del software en las máquinas individuales es sumamente impráctico.

2.4.3.4 Antivirus

Herramienta que tiene por objetivo detectar la mayor cantidad de amenazas informáticas que puedan afectar un ordenador y bloquearlas antes de que la misma pueda infectar un equipo, o poder eliminarla tras la infección.

2.4.3.5 Web Filtering

Todo el contenido de Internet que es leído, enviado o recibido conlleva riesgos inherentes. El acceso de los empleados a Internet continúa incrementando el número de peligros potenciales que podrían impactar negativamente en cuatro formas diferentes:

• **Riesgos en la seguridad**: virus, spyware y otros tipos de malware pueden entrar en la red de una compañía a través de servicios de webmail, la descarga de archivos, el uso indebido de mensajería instantánea, aplicaciones P2P y el acceso a sitios no relacionados con el trabajo.

• **Riesgos legales**: Contenidos inapropiados pueden derivar en asuntos complejos de discriminación u hostigamiento sexual, religioso o étnico. Además, la descarga y distribución de contenidos ilegales a través de la red corporativa puede presentar problemas legales para la compañía.

• **Riesgos de productividad**: Las tentaciones que generan los sitios no relacionados con el trabajo son infinitas. Sólo 20 minutos de navegación "recreacional" pueden costarle a una compañía con 500 empleados más de 8 mil dólares por semana.

• **Riesgos en la red**: Un empleado puede hacer colapsar la red simplemente al ingresar a un sitio web maligno. Otras actividades como la navegación recreacional" o la descarga de archivos en mp3 congestionan la red, reduciendo su performance, afectando de forma negativa los negocios de la empresa.

Para prevenir este tipo de amenazas, existen dos métodos de protección a través de filtros web integrados y redirigidos.

2.4.3.5.1 Filtro Web Integrado

Permite definir políticas de acceso a la Red a través del Firewall, mediante una interfaz gráfica.

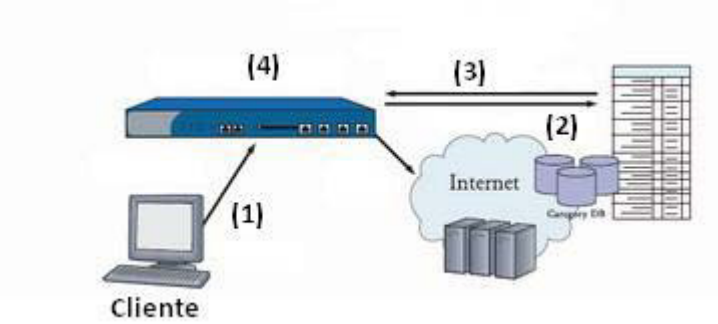


Figura 3.2 Filtrado Web Integrado

Funcionamiento:

1. El cliente inicia una solicitud de URL http.
2. El Firewall intercepta el pedido y chequea el cache del dispositivo para ir en busca de la URL. Si la URL no está en el cache, es enviada al servidor.
3. El servidor responde enviando la categoría a la cual pertenece la URL solicitada, como por ejemplo, "Armas" o "Deportes".
4. El Firewall compara la categoría con los parámetros ingresados por el administrador y permite o bloquea el acceso al site, o bien redirecciona el tráfico a una página interna.
5. En caso de que la URL esté permitida, se garantiza su acceso vía http.

2.4.3.5.2 Filtro Web Redirigido

El Filtro Web Redirigido reúne los pedidos de acceso a la Red del firewall y los envía a un filtro en un servidor web externo para reforzar las políticas de filtrado de la organización.

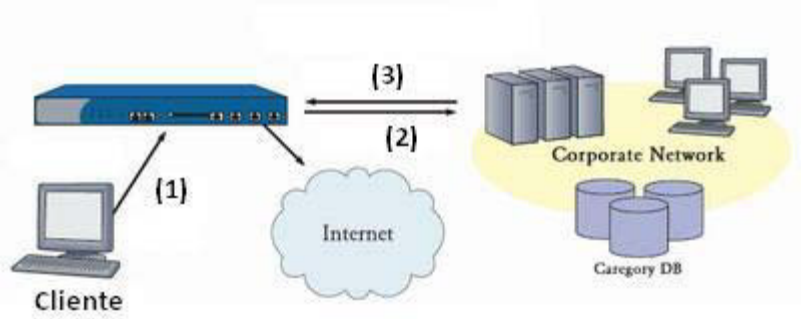


Figura 3.3 Filtro Web Redirigido

Funcionamiento:

1. El cliente inicia una solicitud URL http.
2. El Firewall intercepta el pedido y lo envía al servidor del filtro URL.
3. El filtro web responde según la política establecida para la URL, de acorde a la categoría, como "Armas" o "Deportes" y permite, niega o redirige la solicitud a una página interna.
4. En caso de que la solicitud sea aprobada, el acceso http queda garantizado.

2.4.3.6 Anti-Spam

Para disminuir el número de correos no deseados y los potenciales ataques que acarrean. El motor Anti-Spam actúa como la primera línea de defensa, filtrando e-mails de conocidos spammers y ohishers. Cuando un correo malicioso es recibido, es bloqueado o marcado para que el servidor de correo lleve adelante las acciones correspondientes.

2.4.4 VENTAJAS DE UTM

Las principales ventajas son:

1. Menor complejidad: solución de seguridad individual. Único proveedor. Individual AMC
2. Simplicidad: Evitar la instalación del software y el mantenimiento de servicios múltiples
3. Fácil gestión: Plug & Play Arquitectura, GUI basada en Web para facilitar la gestión
4. Rendimiento : cero horas de protección sin degradar el rendimiento de la red
5. Solución de problemas : Un único punto de contacto - 24 × 7 Asistencia Técnica del Proveedor
6. Reducción de los requisitos de capacitación técnica, un solo producto para aprender.

2.5 IDS / IPS

La protección proactiva de recursos de red es la última tendencia en seguridad de la informática. La mayoría de los Sistemas de Detección de Intrusiones (IDS) supervisar pasivamente la red en busca de signos de actividad intrusiva. Cuando la actividad maliciosa es detectada, el IDS proporciona la capacidad para bloquear la actividad del host sospechoso. Este enfoque reactivo no impide que el tráfico de ataque inicial.[CAR05]

2.5.1 Información General Sobre Prevención De Intrusos

2.5.1.1 Terminología

En la tabla se describe los términos primarios que se utilizan para describir las funcionalidades de la solución del IPS.

Terminología	Descripción
Modo en línea	Examina el tráfico de la red mientras y tiene la posibilidad de detener el tráfico de malicioso lleguen al sistema de destino.
Modo promiscuo	Examina pasivamente el tráfico de red para el comportamiento intrusivo.
Motor de Firma	Un motor que soporta firmas que comparten características comunes (Como el mismo protocolo)
Firma basado en flujo	Firma que pone en marcha sobre la base de la información contenida en una secuencia de paquetes entre dos sistemas (como los paquetes en una red TCP (Conexión).
Firma basada en el Comportamiento	Firma que se activa cuando se desvía el tráfico de comportamiento de los usuarios regulares.
Firma basada en Anomalía	Firma que pone en marcha cuando el tráfico excede a la base configurada.
Falso negativo	Situación en que el IDS/IPS falla para detectar el tráfico aunque hay una actividad maliciosa.
Falso positivo	Una situación en que el IDS/IPS identifica erróneamente la actividad del usuario normal disparando una alarma.
Verdadero negativo	Una situación en la que una firma no se dispara durante el tráfico de usuarios normales en la red.
Verdadero positivo	Una situación en la que el IDS/IPS identifica correctamente el ataque contra la red.
Inspección profunda de paquetes	Decodifica los protocolos y analiza los paquetes para permitir reforzar la política basada en el tráfico del protocolo real.
Correlación de eventos	La asociación de múltiples alarmas o eventos con un solo ataque
Calificación de riesgo (RR)	Nivel de peligrosidad sobre la base de numerosos factores, además de la gravedad del ataque.

Tabla 2.1 Terminología del IPS

EL propósito del IPS / IDS es detectar cuando un intruso está atacando su red. No todo los IDS/IPS, utilizan los mismos mecanismos de disparo para generar alarmas de intrusión. Existen tres grandes mecanismos:

- Detección de anomalías
- Detección de Firmas
- Detección de Protocolo

2.5.1.2 Mecanismos de activación

Se refieren a la acción que hace el IDS / IPS para generar una alarma. Por ejemplo, el mecanismo de activación de una alarma contra robo de casa podría ser una rotura de la ventana. En una red IDS se puede activar una alarma. Todo lo que puede indicar una forma fiable intrusión puede ser utilizado como un mecanismo de disparo.

2.5.1.2.1 Detección de Anomalías

También se refiere a la detección basada en perfiles. Con la detección de anomalías, que deben construir los perfiles que definen lo que la actividad se considera normal. Estos perfiles se definen en un período de tiempo y cualquier cosa que se desvíe de este perfil normal genera una alerta.

La principal ventaja de la detección de anomalías es que las alarmas generadas no se basan en firmas de ataques conocidos. En cambio, se basan en un perfil que define la actividad del usuario normal.

2.5.1.2.2 Detección de Firmas

Busca la actividad intrusiva que coincide con específicos firmas. Estas firmas se basan en un conjunto de reglas que coincidan con los patrones típicos y exploits utilizados por los atacantes para acceder a su red. Algunos de los beneficios de la detección de mal uso son los siguientes:

- Las firmas se basa en la actividad intrusiva conocida
- Los ataques detectados están bien definidos
- Sistema es fácil de entender

- Detecta ataques inmediatamente después de la instalación

2.5.1.2.3 Detección de Protocolo

El mecanismo desencadenante es una variación en la detección de firmas. El IPS / IDS analiza el flujo de datos basados en el funcionamiento normal de un protocolo específico. Por lo tanto, el sistema de intrusión verifica la validez de los paquetes con respecto a la definición de protocolo y luego buscar patrones específicos en los distintos ámbitos del protocolo o carga útil de un paquete. Este análisis se centra en dos áreas principales:

- Verificación de validez de los paquetes
- Comprobación del contenido de la carga útil

Mediante un análisis de protocolo, no solo el tráfico malicioso coincide con un paquete válido para el protocolo en cuestión, también debe contener tráfico malicioso conocido en la carga útil.

2.5.1.3 Tipos de IPS / IDS

Ahora que tiene una comprensión básica de la actividad maliciosa que puede generar alarmas de su sistema de intrusión. Los principales tipos de control del IPS / IDS son las siguientes:

- Basada en el host
- Basado en red

2.5.1.3.1 Basada en el host

El sistema de intrusiones basado en Host comprueba la actividad maliciosa verificando la información en el host o en el funcionamiento del nivel de sistema. Estos sistemas de intrusión examinar muchos aspectos de su anfitrión, tales como llamadas al sistema, los registros de auditoría, mensajes de error, y así sucesivamente.

El IPS / IDS basado en Host, examina el tráfico después de que alcance el objetivo del ataque (suponiendo que el anfitrión es el objetivo), se tiene información de primera mano

sobre el éxito del ataque. Con un sistema de intrusiones basado en red, las alarmas se generan en la actividad intrusiva conocido, pero sólo un sistema de intrusiones basado en host puede determinar si ha tenido éxito o fracaso de un ataque.

2.5.1.3.2 Basado en red

El sistema de intrusiones basado en red examina paquetes que pasan por la red, donde olfatea los paquetes de red y compara contra el tráfico de firmas de actividad maliciosa. Una red basada en IPS comprueba efectivamente el tráfico de red para actividades maliciosas, mientras que funciona como un dispositivo de transmisión de capa 2.

Para ser capaz de ver todos los paquetes en la red, el IDS debe colocar la tarjeta de interfaz de red (NIC) en modo promiscuo. Mientras que en modo promiscuo.

Un sistema de intrusiones basado en red, en comparación con una solución basada en host, tiene los siguientes beneficios:

- Perspectiva general de la red
- No tiene que ejecutarse con cada sistema operativo en la red.

Al ver el tráfico destinado para las máquinas múltiples, un sensor recibe una perspectiva de red en relación con la los ataques contra la red. Si alguien está explorando varios hosts en su red, esta información es evidente para el sensor.

Otra de las ventajas de un sistema de intrusiones basado en red es que no tiene que ejecutarse con cada sistema operativo en la red. En su lugar, un sistema de intrusiones basado en red se basa en un número limitado de dispositivos sensores para capturar tráfico de la red.

2.6 CLUSTER DE ALTA DISPONIBILIDAD

2.6.1 Terminología

Nodo: Dispositivo Terminal, pueden ser estaciones de trabajo o servidores.

Clúster: Consiste en un grupo de nodos conectados entre sí que interactúan como una sola maquina, reduciendo así considerablemente la tolerancia a fallos y caídas de servicio. Un clúster de alta disponibilidad es un conjunto de dos o más máquinas, que se caracterizan porque el fallo en una de las máquinas no hace detenerse el servicio que ofrecen en conjunto.

Caída del Servicio (DOWNTIME): Cualquier suceso que no permite al usuario realizar su trabajo.

Disponibilidad: Es una medida del tiempo en el que un sistema está funcionando de forma normal. La disponibilidad es una de las características de las arquitecturas empresariales que mide el grado con el que los recursos del sistema están disponibles para su uso por el usuario final a lo largo de un tiempo dado.

La disponibilidad depende de los siguientes puntos:

- **Fiabilidad**: Estaciones de trabajo entre otros.
- **Redundancia**: técnica mediante la cual un componente del sistema es duplicado y cualquiera de sus instancias puede ser utilizada en caso de falla.
- **Escalabilidad**: Mantener el nivel de rendimiento aunque aumenten los clientes del sistema.

Medición de la Disponibilidad

La disponibilidad se cuantifica habitualmente a través del índice de disponibilidad, que se obtiene de dividir el tiempo durante el cual el servicio está disponible por el tiempo total de operación.

DISPONIBILIDAD = T.DISPONIBLE / (T.DISPONIBLE + T.INACTIVO)

El índice de disponibilidad, se puede expresar también como un porcentaje. Por ejemplo, si un sistema tiene una disponibilidad de un 99%, a lo largo de un año se mantendrá funcionando aproximadamente 361 días, y tendrá un tiempo de inactividad de 3,6 días. Los fabricantes o proveedores de servicios suelen utilizar este porcentaje en los acuerdos de nivel de servicio (SLA), para clasificar el nivel de disponibilidad que se espera de un sistema.

Porcentaje de disponibilidad	Tiempo de Interrupción Anual	Tiempo de Interrupción Semanal
98 %	7,3 días	3,3 horas
99 %	3,6 días	1,7 horas
99,9 %	8,8 horas	10 minutos
99,99 %	52,5 minutos	1 minuto
99,999 %	5,3 minutos	6 segundos
99,9999 %	31,5 segundos	0,6 segundos

Tabla 2.3 Índice de Disponibilidad

Alta Disponibilidad

La alta disponibilidad es la característica que tiene un sistema para protegerse o recuperarse de interrupciones o caídas, de forma automática y en un corto plazo de tiempo. Los cluster de alta disponibilidad se diseñan para eliminar o tolerar los posibles puntos de fallo, para ello se emplea principalmente la redundancia interna de componentes (red, almacenamiento, fuentes de alimentación, etc.) así como de los elementos de infraestructura (sistema eléctrico, electrónica de red, etc.).

2.6.2 Clúster de alta Disponibilidad

2.6.2.1 Definición

Es un conjunto de dos o más dispositivos, que se caracteriza por compartir el sistema y servicios, y porque están constantemente monitorizándose entre sí. Si se produce un fallo del hardware o de los servicios de alguno de las maquinas que forman el clúster, el software de alta disponibilidad es capaz de re arrancar automáticamente los servicios que han fallado

en cualquiera de los otros equipos del clúster. Y cuando el servidor que ha fallado se recupera, los servicios se migran de nuevo a la máquina original.

La utilización de clústeres no solo es beneficiosa para caídas de servicio no programadas, sino que también es útil en paradas de sistema programadas como puede ser un mantenimiento hardware o una actualización software.
En general las razones para implementar un clúster de alta disponibilidad son: Aumentar la disponibilidad, mejorar el rendimiento, escalabilidad, tolerancia a fallos, recuperación ante fallos en tiempo aceptable, reducir costes, consolidar servidores, consolidar el almacenamiento.

2.6.2.2 Configuraciones de Clúster de Alta Disponibilidad

2.6.2.2.1 Configuración Activo/Activo

Todos los nodos del clúster pueden ejecutar los mismos recursos simultáneamente. Es decir, los nodos poseen los mismos recursos y pueden acceder a estos independientemente de los demás miembros del clúster. Si un nodo del sistema falla y deja de estar disponible, sus recursos siguen estando accesibles a través de los otros nodos del clúster.
La ventaja principal de esta configuración es que los nodos en el clúster son más eficientes ya que pueden trabajar todos a la vez. Sin embargo, cuando uno de los nodos deja de estar accesible, su carga de trabajo pasa a los nodos restantes, lo que produce una degradación del nivel global de servicio ofrecido a los usuarios.
En la siguiente figura se muestra como ambos nodos están activos, proporcionando un mismo servicio a los diferentes usuarios. Los clientes acceden al servicio o recursos de forma transparente y no tienen conocimiento de la existencia de varios nodos formando un clúster. En la figura 3.6 se muestra el funcionamiento.

2.6.2.2.2 Configuración Activo/Pasivo

Consiste en un nodo que posee los recursos del clúster y otros nodos que son capaces de acceder a esos recursos, pero no los activan hasta que el propietario de los recursos ya no esté disponible.

Las ventajas de la configuración activo/pasivo son que no hay degradación de servicio y que los servicios solo se reinician cuando el servidor activo deja de responder. Sin embargo, una desventaja de esta configuración es que los nodos pasivos no proporcionan ningún tipo de recurso mientras están en espera, haciendo que la solución sea menos eficiente que el clúster de tipo activo/activo. Otra desventaja es que los sistemas tardan un tiempo en migrar los recursos (failover) al nodo en espera.

Figura 3.4 Alta Disponibilidad configuración Activo - Activo

Figura 3.5 Alta Disponibilidad configuración Activo - Pasivo

2.6.2.3 Funcionamiento de un clúster de alta disponibilidad

En un clúster de alta disponibilidad, el software de clúster realiza dos funciones fundamentales. Por un lado intercomunica entre sí todos los nodos, monitorizando continuamente su estado y detectando fallos. Y por otro lado administra los servicios ofrecidos por el clúster, teniendo la capacidad de migrar dichos servicios entre diferentes servidores físicos como respuesta a un fallo.

A continuación se describen los elementos y conceptos básicos en el funcionamiento del clúster.

- **Recurso y Grupos de Recursos**

  Tradicionalmente se entiende como servicio a un conjunto de procesos que se ejecutan en un momento dado sobre un servidor y sistema operativo. Este último provee a los procesos de los recursos necesarios para realizar su tarea: sistema de ficheros, interfaces de red, tiempo de CPU, memoria, etc.

  En un clúster de alta disponibilidad, el software de clúster, abstrae e independiza a los servicios de un host concreto. Posibilitando que estos se desplacen entre diferentes nodos de forma trasparente para la aplicación o los usuarios.

- **Intercomunicación**

  El software de clúster gestiona servicios y recursos en los nodos. Pero además, tiene que mantener continuamente entre estos una visión global de la configuración y estado del clúster. De esta forma, ante el fallo de un nodo, el resto conoce que servicios se deben restablecer.

- **Heartbeat**

  El software de clúster conoce en todo momento la disponibilidad de los equipos físicos, gracias a la técnica de heartbeat. El funcionamiento es sencillo, cada nodo informa periódicamente de su existencia enviando al resto una “señal de vida”.

- **Escenario Split-Brain**

  En un escenario split-brain, más de un nodo o aplicación pertenecientes a un mismo clúster intentan acceder a los mismos recursos, lo que puede causar daños a dichos recursos. Este escenario ocurre cuando cada nodo en el clúster cree que los otros nodos han fallado e intenta activar y utilizar dichos recursos.

- **Monitorización de Recursos (Resource Monitoring)**

  Ciertas soluciones de clustering HA permiten no solo monitorizar si un host físico está disponible, también pueden realizar seguimientos a nivel de recursos o servicios y detectar el fallo de estos.

- **Reiniciar Recursos**

  Cuando un recurso falla, la primera medida que toman las soluciones de clúster es intentar reiniciar dicho recurso en el mismo nodo. Lo que supone detener una aplicación o liberar un recurso y posteriormente volverlo a activar.

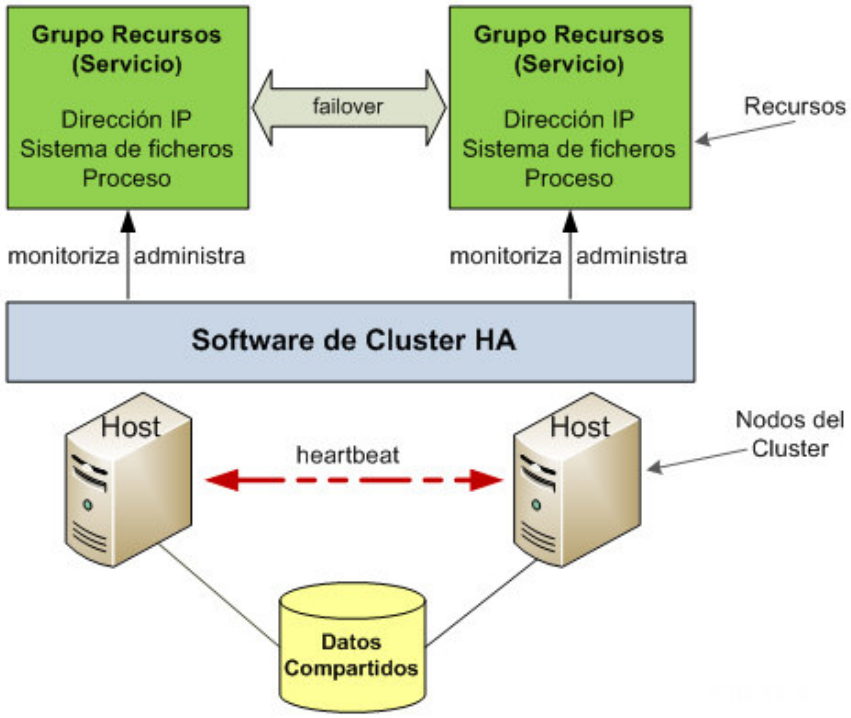


Figura 3.6 Funcionamiento de un clúster de alta disponibilidad

- **Migración de Recursos (Failover)**

  Cuando un nodo ya no está disponible, o cuando un recurso fallido no se puede reiniciar satisfactoriamente en un nodo, el software de clúster reacciona migrando el recurso o grupo de recursos a otro nodo disponible en el clúster.

  De este modo el tiempo de inactividad por el posible fallo es mínimo, y el clúster seguirá proporcionando el correspondiente servicio.

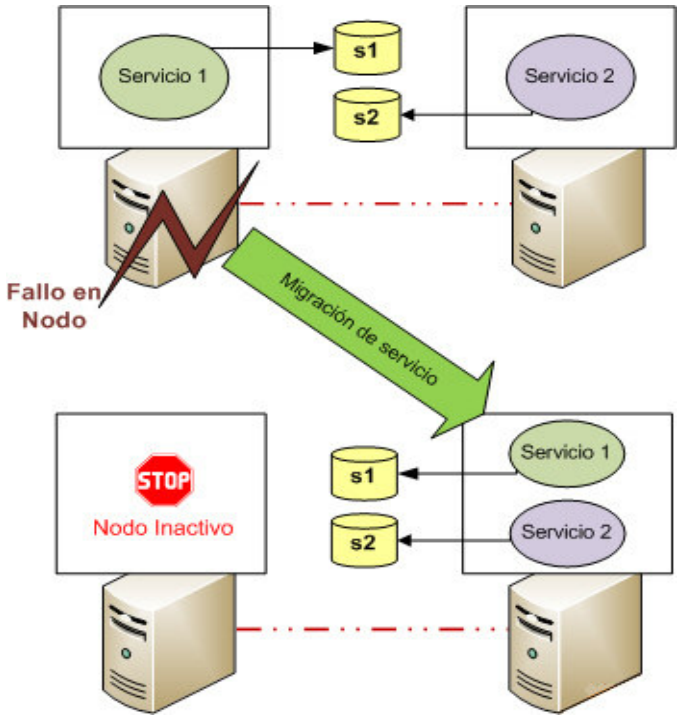


Figura 3.7 Migración de recursos

- **Dependencia entre recursos**

  Habitualmente para que el clúster proporcione un servicio, son necesarios no solo un recurso si no varios (IP virtual, sistema de ficheros, proceso), lo que se conoce como grupo de recursos. Cuando se arranca o detiene un servicio, sus recursos tienen que activarse en el orden apropiado ya que unos dependen de otros. El software de clúster tiene que permitir definir estas dependencias entre recursos así como entre grupos.

- **Preferencia de Nodos**

  En configuraciones de clúster con múltiples nodos, es común distribuir los servicios a proporcionar entre los diferentes servidores. Además puede que los servidores tengan características hardware diferentes (CPU, memoria Ram) y nos interese que, para un estado ideal del clúster, determinados servicios se ejecuten siempre en un determinado servidor.

  Este comportamiento se define mediante la preferencia de nodo en la definición de cada recurso.

- **Comunicación con otros sistemas**

  El clúster tiene que monitorizar no solo que un servidor y sus servicios están activos, también debe de comprobar que, dicho servidor no se encuentre desconectado de la red por el fallo de un switch, etc. Por lo tanto el software de clúster debe comprobar que los nodos son alcanzables. Un método simple para conseguirlo, es verificar que cada nodo tiene accesible el router o puerta de enlace de la red de usuarios.

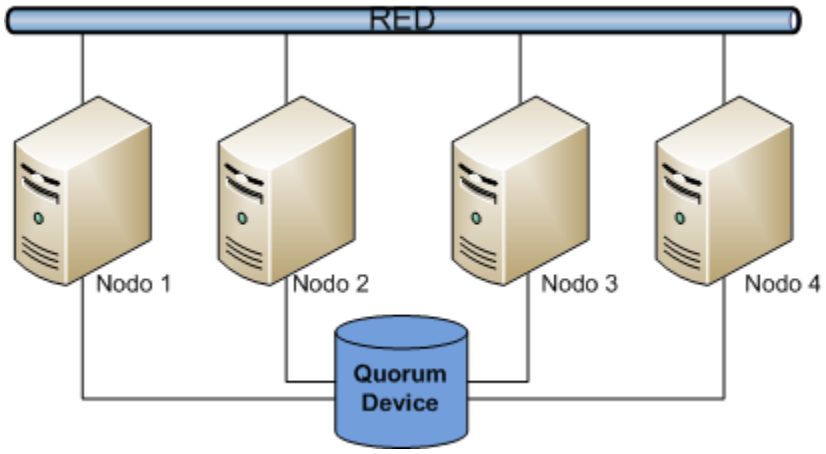


Figura 3.8 Quorum

2.7 Calidad de Servicio (QoS)

En una red donde convergen diferentes tipos de aplicaciones, tales como voz, video y datos, las características de cada uno de los tráficos son muy diferentes. El tipo de flujo clasificado como "datos" que puede ser retransmitido. Tales son los casos de los e-mails, la navegación Web, transferencia de archivos, etc. El protocolo utilizado en la capa de transporte para estos casos es generalmente TCP, el cual provee un mecanismo de detección de errores y pérdida de información que brinda la posibilidad de la retransmisión de aquellos paquetes perdidos o erróneos. Por otro lado el flujo clasificado como "real time" que se refiere a tipo de aplicaciones de voz y de video, es todo aquel que utiliza UDP como protocolo y que por ende no dispone de retransmisión de paquetes. Es por eso que un paquete de voz o video digitalizado no se retransmite bajo ninguna condición.

Actualmente las redes convergentes enfrentan desafíos:

1. **Ancho de banda recurso finito:** Teniendo un solo enlace físico para poder brindar los distintos servicios, hará que los paquetes de cada uno de ellos compitan por el ancho de banda (BW) contratado. Esto provocará que el uso del enlace por parte de uno de los tipos de tráfico reste BW para el otro.
2. **End-to-end Delay:** El tiempo total que le toma a los datos o paquetes de voz para llegar a su destino. Es decir, retardo que un paquete de voz sufre desde que se generó en el equipo que digitalizó la misma hasta la llegada en el equipo destino.
3. **Jitter**: El peor enemigo de la calidad de voz es el Jitter (o variación del delay). Mientras que un Delay constante provoca un retardo en la escucha del interlocutor, el Jitter provoca una deformación de la palabra que la vuelve inteligible.

   Los factores que contribuyen al end-to-end delay (o retardo total en el enlace) son:

   a. Tiempo de propagación del enlace (aire, fibra óptica, par de cobre, etc.)
   b. Retardo por serialización (tiempo que el equipo de transmisión tarda en "poner" el paquete en el enlace.)
   c. Procesamiento y/o encolado (El tiempo que tarda un router en procesar el paquete).
4. **Pérdida de paquetes**: Es la congestión del enlace.

2.7.1 Definición de QoS

QoS es la capacidad de la red para proporcionar un mejor o servicio especial a un conjunto de usuarios, aplicaciones o ambos.

2.7.2 Implementar QoS

Implica tres pasos principales:

1. Identificar los tipos de tráfico y sus requisitos
2. Clasificación de tráfico basado en las necesidades identificadas
3. Definir las políticas para cada clase de tráfico

El primer paso en la aplicación de QoS en una empresa es estudiar y descubrir los tipos de tráfico y definir los requerimientos de cada tipo de tráfico identificado. Si dos, tres, o más tipos de tráfico tienen los mismos importancia y necesidades, no es necesario definir muchas clases de tráfico. La clasificación de tráfico, que es el segundo paso en la implementación de QoS, definirá unas pocas clases de tráfico. Las aplicaciones que terminan en diferentes clases de tráfico tienen diferentes necesidades; por lo tanto, la red debe proporcionarles tipos de servicios diferentes. Los tres pasos de la aplicación de QoS en una la red se explican a continuación: [RAN07]

2.7.2.1 Identificar los tipos de tráfico y sus requisitos

La identificación de los tipos de tráfico y sus necesidades, el primer paso en la aplicación de QoS, se compone de los siguientes elementos:

- Auditoría del desempeño de red
- Determinar la importancia de cada aplicación de acuerdo a los objetivos del negocio, partir de eso, puede derivar la definición de las clases de tráfico y los requisitos para cada clase. Este paso comprueba si retrasar o descartar paquetes de cada solicitud es aceptable.
- Definir los niveles de servicio apropiados para cada clase de tráfico, se definen los recursos como ancho de banda, retardo máximo garantizado de extremo a extremo, jitter.

2.7.2.2 Clasificación de tráfico basado en las necesidades identificadas

Se puede clasificar el tráfico o tipos de aplicación dentro de la misma clase que deberán tener requisitos empresariales comunes:

- El tráfico de voz (VoIP) de clase de voz tiene requisitos específicos de ancho de banda, y su retardo debe ser eliminadas o al menos minimizado. Por lo tanto, esta clase tiene la más alta prioridad, pero que tiene ancho de banda limitado.
- El tráfico de aplicaciones de misión crítica
- El tráfico de señalización, como el establecimiento de llamada de voz.
- El tráfico de aplicaciones transaccionales, como la base de datos, ERP y SAP.
- El tráfico del Mejor esfuerzo, Todos los tipos de tráfico no definido se consideran mejor esfuerzo y recibir el resto de ancho de banda en una interfaz.
- Tráfico Scavenger, Esta clase de aplicaciones será asignado a una clase y se determinado ancho de banda limitado. Esta clase se considera inferior a la clase del tráfico del mejor esfuerzo.

2.7.2.3 Definición de Políticas para cada Clase de tráfico

Después de las clases de tráfico se han formado sobre la base de la auditoría de las redes y los objetivos de negocio, el paso final de la aplicación de QoS en una empresa es proporcionar una definición del nivel de servicio que debe asignarse a cada clase de tráfico. Esto se conoce como la definición de una política de calidad de servicio, y podría incluir tener que realizar las siguientes tareas:

- Establecer un límite máximo ancho de banda para una clase.
- Configurar el ancho de banda mínimo garantizado para una clase.
- La asignación de un nivel de prioridad en relación con una clase.
- Aplicar la gestión de la congestión, evitar la congestión.
- tecnologías para una clase.

2.7.3 Modelos de QoS

Esta sección trata sobre los tres modelos de calidad de servicio: la mejor esfuerzo, de servicios integrados, y Servicios diferenciados.

2.7.3.1 Modelo de Mejor Esfuerzo

Significa que no existe una política de QoS que se aplica. Es natural preguntarse por qué esta modelo no fue llamado ningún esfuerzo. Dentro de este modelo, los paquetes que pertenecen a las llamadas de voz, correos electrónicos, archivos transferencias, etc. Tienen la misma importancia y, de hecho, estos paquetes no son ni siquiera diferenciados.

Beneficios de este modelo:

- El Internet es una red de mejor esfuerzo. El modelo de "mejor esfuerzo" no tiene capacidad de ampliación límite. El ancho de banda de las interfaces de router determina la eficiencia de procesamiento.
- No requiere ninguna configuración especial de QoS, por lo que es más fácil y más rápida de aplicar este modelo.

Las desventajas del modelo:

- No ofrece ninguna garantía acerca del ancho de banda disponible.
- No distingue los paquetes que pertenecen a las aplicaciones que tienen diferentes niveles de importancia.

2.7.3.2 Modelo de Servicios Integrados

Los Servicios Integrados (IntServ), se basa en explícita de señalización, gestión y reserva de recursos de red para las aplicaciones que necesitan y exigirlo. IntServ se refiere a menudo como Hard-QoS, porque garantiza características tales como ancho de banda, retardo y pérdida de paquetes, proporcionando así un nivel de servicio predecible. IntServ imita el modelo de PSTN, donde cada llamada implica de la señalización de extremo a extremo y asegurar los recursos a lo largo de la ruta del origen al destino. Debido a que cada aplicación puede hacer una única solicitud, IntServ es un modelo que puede ofrecer un nivel de múltiples servicios.

Para una implementación exitosa de IntServ:

- **Control de admisión,** responde a las solicitudes de admisión de recursos de extremo a extremo los recursos. Si los recursos no se puede proporcionar sin afectar a las aplicaciones existentes, la solicitud es rechazada.
- **Clasificación**, El tráfico que pertenece a una aplicación que ha hecho una reserva de recursos debe ser clasificados y reconocidos por los routers de tránsito para que puedan proporcionar servicios apropiados a esos paquetes.
- **Monitorizar**, es importante medir y vigilar que las solicitudes no excedan de los recursos. Dependiendo de si una solicitud se ajusta o supera los recursos, se adoptaran medidas adecuadas.
- **Cola de servidor,** es importante que los dispositivos de red a ser capaz de procesar paquetes y otros de reenvío.
- **Planificación**

Beneficios de este modelo:

- Control de admisión de recursos explícito de extremo a extremo
- Control de política de solicitud de admisión.
- Señalización de puerto dinámico.

Las desventajas del modelo:

- Cada flujo de activos tiene una señalización continua. Esta sobrecarga puede ser circunstancialmente mayor que el número de flujos crece.
- Debido a que cada flujo es rastreados y mantenidos, IntServ basado en los flujos no se considera escalable para implementaciones de gran tamaño, como Internet.

2.7.3.3 Modelo de servicios diferenciados

Los Servicios Diferenciados (DiffServ) es el más nuevo de los tres modelos de calidad de servicio, y tiene su desarrollo destinado a superar las limitaciones de sus predecesores. DiffServ no utiliza la señalización, y se basa en el comportamiento por salto (per hop

behavior - PHB). PHB significa que cada salto en una red debe ser pre programado para proporcionar un nivel de servicio para cada clase de tráfico. PHB, no requiere de señalización, siempre y cuando el tráfico es marcado para ser identificados como una de las clases de tráfico previsto. Este modelo es más escalable Esto significa que incluso si miles de flujos se activan, este modelo esta ría en la capacidad de categorizarlos según las clases predefinidas.

Con el modelo DiffServ, el tráfico primero es clasificado y marcado. DiffServ puede proteger la red de sobre suscripción mediante el uso de técnicas de control de admisión y políticas de calidad de servicio.

Beneficios de DiffServ:

- Escalabilidad.
- Capacidad de dar soporte a múltiples niveles de servicio diferente.

Desventajas de DiffServ:

- No puede ofrecer una garantía absoluta de servicio, por ello que se asocia con el término QoS Soft.
- Se requiere la aplicación de complejos mecanismos a través de la red.

2.7.4 Mecanismos de QoS

Los distintos mecanismos de QoS son los que en conjunto hacen posible la implementación de la Calidad de Servicio en redes IP. Estos mecanismos, deben ser llevados a cabo en un cierto orden tal como si fuera una cadena de producción industrial. [GRA07a]

Figura 3.9 Mecanismos de QoS

2.7.4.1 Clasificación

El clasificado de tráfico es la identificación de un cierto tipo de flujo y puede ser basado en una cierta interfaz de entrada. Esta opción si bien es simple no es muy flexible por lo que una de las opciones más comunes es definir una lista de acceso (Access List) y establecer el criterio con el cual se pueda identificar al tráfico.

2.7.4.2 Marcado

Una vez que puedo clasificar e identificar el tipo de tráfico puedo tomar la siguiente acción que no afecta inmediatamente al tráfico, el marcado que consiste en establecer un valor o etiqueta a este campo.

2.7.4.3 Policing y Shaping

Para poder hacer una restricción o manejo del ancho de banda (BW) los mecanismos utilizados son policing y shaping. Si bien las traducciones literales son "custodiando" y "dando forma" respectivamente, la diferencia entre ellos es que policing no tiene en cuenta el comportamiento del tráfico mientras que shaping sí lo hace, por lo que la reacción a la violación de los límites establecidos es distinta para cada uno de estos ellos.

Policing, Puede ser aplicado tanto en la entrada del equipo como en la salida y su funcionamiento está basado en un valor límite de cantidad de información transmitida por unidad de tiempo. Este límite (establecido en bits por segundo o Bytes por segundo) es fijado en la configuración del equipo y en cuanto el tráfico entrante o saliente de la interfaz alcanza este límite, los paquetes que los sobrepasan sufren la acción configurada para tal caso. Esta acción pueden ser transmitidos, descartados o remarcados.

Shaping, Puede ser aplicado solamente a la salida de los equipos, tiene en cuenta la posibilidad de que el flujo de información pueda tener picos de tráfico llevados a cabo por ráfagas de esta información. Estas ráfagas de información serían descartadas o bien remarcadas a una calidad inferior si el mecanismo utilizado a la salida fuera Policing.
La implementación más básica de shaping establece entonces dos límites, uno por encima del cual los paquetes son almacenados en las colas de salida para luego ser transmitidos, y

otro por encima del cual son directamente descartados. La diferencia entre estos dos límites es el tamaño de ráfaga de información permitida. Este mecanismo no castiga tan duramente al tráfico y evita un comportamiento del flujo de tipo diente de sierra generado por el protocolo TCP.

Cualquier persona pensaría que shaping es un mecanismo muy superior a policing ya que es mucho más efectivo en cuanto al aprovechamiento del ancho de banda, pero sería una conclusión apresurada si no se tuviera en cuenta que para poder aprovechar el ancho de banda se está agregando delay. Los paquetes que con policing serían descartados están siendo almacenados en las colas de salida y el tiempo de espera en estas colas es directamente el delay agregado.

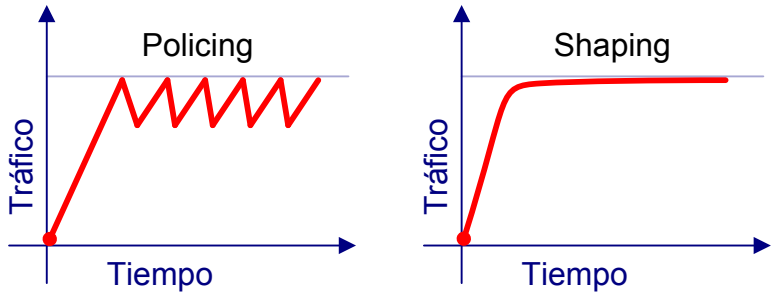


Figura 4.0 Policing y Shapping

En la figura 4.5 se puede ver el comportamiento del tráfico cercano a los límites configurados, en función del tiempo para los mecanismos policing y shaping.

La diferencia entre Policing y shaping

Policing puede ser aplicado en la entrada y en la salida del equipo y su funcionamiento está basado en un valor límite de cantidad de información transmitida por unidad de tiempo. Shaping puede ser aplicado solo a la salida de los equipos y tiene en cuenta la posibilidad de que el flujo de información puede tener picos de tráficos llevados a cabo por ráfagas de esta información.

2.7.4.4 Administración de la congestión

Los últimos dos mecanismos presentados en la cadena de QoS describen la manera de despachar los paquetes por la interfaz de salida y cómo, en caso de tener congestión (llegar al límite físico de transmisión de la interfaz o del tamaño de la memoria asignada a dicha interfaz) evitarla de alguna manera.

Los paquetes despachados son tomados de las colas de salida, y para eso se deberá definir algún criterio de elección de colas ya que en caso de elegir siempre la misma, cierto tráfico que permanece en las colas no atendidas permanecerán un tiempo elevado en las mismas. Estos criterios y formas de atender las colas de salida son definidos "métodos de atención de colas" [GRA07b].

2.7.4.4.1 Métodos de atención de colas

2.7.4.4.1.1 FIFO

Cuando se dispone de una sola cola de salida, el primer paquete despachado es aquel que fue el primero en ingresar a dicha cola. Esa modalidad es denominada FIFO (First IN First OUT) y es la más simple que se pueda encontrar, pero una vez que la cola esté llena todos los paquetes entrantes serán descartados. Esto no nos permite diferenciar el trato que se le podría dar a los paquetes marcados con diferentes calidades de servicio. Este fenómeno de descarte de todos los paquetes entrantes cuando la cola se llena es conocido como tail-drop.

2.7.4.4.1.2 Colas Priorizadas (Priority Queues)

Para poder priorizar el tráfico de las más altas calidades se utilizan colas llamadas de alta prioridad o Priority Queue (PQ). Para esto se necesita que haya un mínimo de dos colas de salida para que el tráfico marcado con la clase que se quiera priorizar sea colocado en la PQ y el resto del tráfico en la cola restante o bien demás colas restantes. La regla que hace efectiva la priorización es que mientras haya algún paquete en la cola PQ, este deberá ser despachado por la interfaz de salida y solo se tomarán paquetes de las demás colas en ausencia de tráfico en la PQ. De esta manera en cuanto exista algo de tráfico de la calidad definida para la PQ, este será despachado, mientras que el resto del tráfico deberá esperar para ser atendido. Como ventaja inmediatamente visible es el poco tiempo que deben esperar los paquetes de la calidad definida para la PQ, por lo que generalmente el tráfico

que se destina a la PQ es tráfico sensible a la latencia como puede ser los flujos “real time”. Por esto es que esas colas son llamadas también de “baja latencia”.
Como gran desventaja de esto es el gran tiempo que deben esperar los paquetes de las demás colas, llegando este a ser infinito en caso de un excesivo y constante tráfico de la más alta calidad.

2.7.4.4.1.3 Round Robin

Round Robin es el nombre en inglés que recibe la modalidad que atiende distintas colas una a una de manera alternada y en forma de ronda (como ejemplo se puede tomar una baraja entre varios jugadores). Esta atención equitativa de las colas hace que el ancho de banda disponible sea compartido por igual entre todas las colas de salida. Para asignar las colas a cada una de las calidades de servicio se deberá tener en cuenta esta forma de compartir el ancho de banda.
Ejemplo: disponemos de ocho calidades de servicio, cuatro colas de salida y la modalidad de despacho es Round Robin. Agrupando de a dos calidades consecutivas en cada una de las colas, la cola 1 tendrá las calidades 1 y 2, la cola 2 la 3 y 4 y así sucesivamente. De esta manera cada uno de los grupos de calidades (1 y 2, 3 y 4, etc.) tendrán el 25 por ciento del ancho de banda del enlace (al tener 4 colas, a cada una de ellas le corresponde un 25 por ciento). Con este método la administración del ancho de banda para cada calidad se vuelve compleja pero flexible.

2.7.4.4.1.4 Round Robin ponderado o Weighted Round Robin (WRR)

El Weighted Round Robin (WRR) permite definir un peso a cada una de las colas haciendo que la ponderación de las colas no sea uniforme tal como se explico en el punto anterior. De esta manera se facilita la administración del ancho de banda para cada una de las calidades.
Si además la cantidad de colas coincide con la cantidad de calidades de servicio que quiero brindar, el cálculo del ancho de banda para cada una de estas calidades es inmediato. La ponderación podrá ser realizada en cantidad de paquetes o porcentaje de ancho de banda del total del enlace, traduciéndose este último en Bytes transmitidos.

2.7.4.4.1.5 Déficit Round Robin (DRR)

Uno de los problemas de WRR es que cuando la ponderación es realizada por Bytes transmitidos puede existir una imprecisión en el control del ancho de banda debido a que si cuando el anteúltimo paquete transmitido no llegó al límite de los Bytes permitidos pero la diferencia con respecto a este límite no es muy grande, la transmisión del próximo paquete lo excederá ampliamente.

Ejemplo: el MTU es 300 y el límite de Bytes para una cola es de 600Bytes (dos paquetes con MTU). El primer paquete en cola es de 300Bytes pero el segundo y el tercero son de 250Bytes. La suma de los dos primeros paquetes dará un resultado de 550Bytes, resultado que no supera el máximo de 600Bytes, por lo que se transmitirá el tercer paquete. De esta manera en esa ronda para esa cola se habrá transmitido 800Bytes (200Bytes de más con respecto al límite).

Un mecanismo para contrarrestar este efecto es guardar en una variable esos 200Bytes de más que le fueron otorgados a esa cola en esa ronda y restárselos en la siguiente. Con lo que el límite para la siguiente ronda será de 400Bytes.

De esa manera en algunas rondas se sobrepasará el límite y en otras no será alcanzado, dando como resultado promedio un número cercano al límite real.

2.7.4.4.1.6 Random Early Detection (RED)

Supongamos que tenemos solamente una cola de salida y que es del tipo FIFO. Cuando el tráfico llegue al límite del impuesto por la interfaz física, se empezarán a descartar los últimos paquetes que entran en la cola. Este efecto tail-drop provocará que alguno de los extremos de la conexión TCP baje su tráfico drásticamente tal como fuera explicado anteriormente. Si el descarte de paquetes es significativamente grande afectará entonces a muchas o bien todas las conexiones existentes, teniendo como consecuencia que la totalidad del tráfico realicen la disminución en simultáneo. Este fenómeno en la que todas las conexiones TCP disminuyen el tráfico notoriamente es conocido como sincronización TCP.

Para poder evitar este fenómeno se buscó un método que afecte solo a algunos extremos TCP, para que estos disminuyan el tráfico mientras que el resto siga enviando tráfico normalmente. Para poder lograr dejar que cierto tráfico continúe normalmente es necesario

actuar antes de la congestión y es por eso que se habla de la detección temprana de la congestión. Este método conocido en inglés como Random Early Detection (RED) utiliza un valor umbral de tráfico por encima del cual comienza a descartar paquetes de manera aleatoria. Esta aleatoriedad (porcentaje de paquetes descartados) en conjunto con el umbral son los parámetros básicos a ser configurados en cualquier implementación.

Ejemplo: un enlace de 256Kbps podría tener configurado un umbral de 196Kbps y un porcentaje de descarte del 40 por ciento. Esto significa que cuando el tráfico llegue a 196Kbps se descartarán 40 paquetes cada 100 despachados. Las conexiones TCP que disminuyan su tráfico serán aquellas cuyos paquetes estén dentro de esos 40 descartados y los que se encuentren en los 60 restantes mantendrán su tráfico intacto.
El problema de este tipo de implementaciones es que si el tráfico sigue aumentando llegará el momento en que se vuelva a realizar un descarte de la totalidad de lo paquetes de manera abrupta. Es por eso que en algunas implementaciones más complejas es necesario definir dos umbrales y una probabilidad de descarte. Al cruzar el primer umbral, la probabilidad de descarte será mínima y comenzará a aumentar linealmente conforme aumente el tráfico. La pendiente de la función lineal será determinada por el segundo umbral, ya que en ese valor la probabilidad de descarte será el asignado por configuración. Una vez cruzado el segundo umbral, la totalidad del tráfico será descartado. En la figura 1 se puede ver lo explicado.

Este mecanismo explicado en detalle puede ser aplicado para cada una de las colas de salida. Si tenemos la posibilidad de tener una cola de salida para cada una de las calidades de servicio, se podrá aplicar RED indirectamente a cada una de las calidades. Configurando umbrales más pequeños para las calidades más bajas, se podrá evitar la congestión global castigando más duramente a estas, y dar así lugar a que las calidades más altas puedan aprovechar el ancho de banda total.

CAPITULO III:
ESTADO DE ARTE

3.1 Tecnología de equipos UTM

En este punto nos centraremos en las tecnologías que se emplean en la implementación de los equipos UTM, ya que los servicios o componentes que disponen se explicó en el capitulo 2, marco teórico.

3.1.1 Arquitectura de la Primera Tecnología

En esta arquitectura se utiliza una combinación poderosa de software y hardware basada en el uso de "Circuitos Integrados de Aplicación Específica", conocidos por sus siglas en inglés como ASIC, a través de la cual es capaz de ofrecer el procesamiento y análisis del contenido del tráfico de la red sin que ello suponga ningún impacto en el rendimiento de las comunicaciones.
La tecnología incluye el Procesador FortiASIC™ y el Sistema Operativo FortiOS™ y son la base del alto rendimiento ofrecido por los equipos. [WEB 05]

FortiASIC™
La exclusiva arquitectura basada en ASIC, permite el análisis del contenido del tráfico en tiempo real, satisfaciendo todas las necesidades de protección a nivel de aplicación sin impactar en el rendimiento de la red.
El procesador FortiASIC™ posee múltiples características que hacen posible su alto rendimiento:

- Contiene un motor hardware que acelera el análisis de las cabeceras de cada paquete y del contenido ensamblado de los paquetes de una conexión, acelerando de este modo los procesos del motor del Firewall y del motor de IDS/IPS al ser capaz de identificar a velocidad de línea el flujo al que pertenece cada paquete.

- Posee un potente motor de comparación de firmas que permite comparar el contenido del tráfico de una sesión contra miles de patrones de firmas de virus, ataques de intrusión, u otros patrones sin comprometer el rendimiento de la red. Este motor de análisis reensambla los paquetes pertenecientes a un mismo mensaje

en memoria, carga las firmas necesarias y realiza una búsqueda por comparación de patrones, todos estos procesos se realizan a nivel de hardware con la ganancia en velocidad que eso supone.

- El chip FortiASIC™ incluye también un motor de aceleración de cifrado que permite realizar cifrado y descifrado de alto rendimiento para el establecimiento de las Redes Privadas Virtuales o VPN.

Figura 4.1 Chip FortiASIC

Aceleración hardware para puertos de red: NP2

El trabajo que realiza un firewall "statefull inspection" para procesar el tráfico de la red está basado en la inspección completa de las cabeceras a nivel 3 y 4 (IP, TCP/UDP), la sustitución de IP's cuando se habilita NAT, el seguimiento del tráfico a través de las tablas de estado y las decisiones de enrutamiento para que el tráfico llegue a su destino, permitiendo sólo las conexiones legítimas a nivel de política así como todo el tráfico que de estas se pueda derivar en protocolos que utilizan varias conexiones como es el caso de FTP o los protocolos de voz.

Este trabajo debe ser realizado independientemente del payload del protocolo en cuestión y para cada uno de los paquetes que compongan una sesión a nivel de aplicación.

Cuando los protocolos en uso se basan en una gran cantidad de paquetes con un payload bajo, el trabajo que ha de llevarse acabo en el dispositivo de firewall es mucho mayor, ya

que este depende exclusivamente de la cantidad y no del tamaño de los paquetes y debido a que en un mismo volumen de datos se han de procesar un número mucho mayor de cabeceras y entradas de las tablas de estado así como de decisiones de enrutamiento. Esta circunstancia, provoca que los equipos que sólo utilizan CPU's de propósito general para realizar las tareas necesarias puedan verse seriamente afectados ante estos tipos de tráfico, llegando a disminuir su rendimiento de tal forma que se introducen retardos en la red e incluso es necesario descartar paquetes debido a la saturación de la CPU del equipo. Esta saturación provoca retardos inadmisibles en determinados protocolos y además afecta al resto del tráfico de la red haciendo que la calidad del servicio se vea afectada muy negativamente.

Queda entonces patente que el troughput de un equipo está directamente relacionado con el tipo de tráfico que se está generando en la red y no sólo con su volumen, y que además, los números comúnmente expuestos en las hojas de producto son imposibles de alcanzar en entornos de tráfico característico de aplicaciones multimedia y convergencia IP como pueden ser el streaming de video o los protocolos RTP para VoIP.

La solución en este tipo de entornos, pasa por el uso de tecnologías de aceleración hardware que doten a los equipos de la capacidad necesaria para llevar a cabo la gestión de las cabeceras de forma rápida y sin influir en el trabajo de la CPU principal, liberando a esta de la carga del procesamiento de las cabeceras de los paquetes, el mantenimiento de las tablas de estado o las decisiones de enrutamiento.
Para cumplir con este requerimiento, se incluye a los dispositivos UTM de aceleradores de puertos (FortiAccel) FA2 o NP2 (Network Processor).

Mediante el uso de circuitos integrados de aplicación específica (ASIC) que dan servicio exclusivo a este tipo de puertos, se acelera la inspección de paquetes a nivel del propio puerto, liberando a la CPU e imprimiendo velocidad de línea a las transmisiones que los atraviesan, sea cual sea el tamaño de paquete utilizado. De esta forma, se puede mantener un troughput continuo de forma optimizada en las comunicaciones, de manera que el nivel

de servicio de los protocolos más sensibles, y por extensión el resto de tráfico de la red, no se vea afectado.
Esta tecnología diferencial, hace que las redes puedan seguir funcionando con normalidad ante protocolos que hacen uso extensivo de paquetes pequeños, como los asociados a los protocolos de VoIP, las aplicaciones multimedia o el tráfico de sincronización de los motores de base de datos.

El núcleo de esta tecnología consiste en el uso de un ASIC, NP2 para dar servicio a varios puertos de red de un equipo, así será el ASIC (NP2) y no la CPU principal o FortiASIC, el que lleva a cabo el procesamiento de los paquetes que entran en cada puerto acelerado, haciendo que la transmisión de estos se realice de forma inmediata sin tener que esperar ciclos de liberación de la CPU principal.

Además, existen varios módulos de expansión con formato AMC que incluyen puertos acelerados, esos módulos pueden contener 4 (ASM-FB4) u 8 (ASM-FB8) puertos GigabitEthernet con interfaz de cobre o 2 (ADM-XB2) puertos 10GigabitEthernet con interfaz SFP**.**

Figura 4.2 Módulos de Expansión ACM

FortiOS™

El sistema operativo FortiOS™ fue diseñado con objeto de soportar funcionalidades de conmutación de alto rendimiento. El núcleo de FortiOS™ es un kernel dedicado, optimizado para procesamiento de paquetes y trabajo en tiempo real. Provee además de un interfaz homogéneo para cada una de las funcionalidades ofrecidas. Este sistema operativo

funciona sobre diversos modelos de procesadores de propósito general, contando con biprocesadores en los equipos de gama alta.

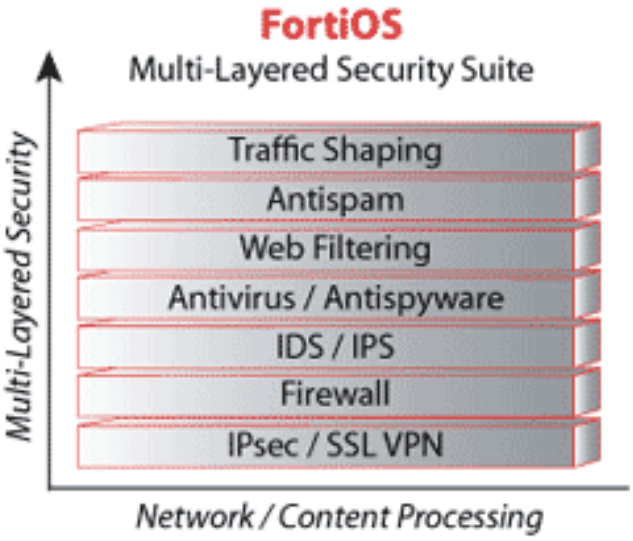


Figura 4.3 Suite Multicapa - FortiOS

3.1.2 Arquitectura de la Segunda Tecnología

Es la primera solución del mercado de Gestión unificada de amenazas (UTM) con arquitectura multinúcleo que ofrece Reassembly-Free Deep Packet Inspection™ de clase empresarial sin impactar significativamente en el rendimiento de la red. Los dispositivos con esta tecnología combinan un potente firewall de inspección profunda de paquetes con una tecnología de protección multicapa y prestaciones de alta disponibilidad.

Fueron diseñados para ser los dispositivos multifuncionales de gestión de amenazas de mayor rendimiento, escalabilidad y fiabilidad. Esto se debe a su arquitectura multinúcleo, que permite el procesamiento en paralelo garantizando una protección ultra rápida y un elevado nivel de escalabilidad. La prestación Application Firewall se compone de un conjunto de herramientas de protección personalizables que permiten a los administradores controlar el tráfico de la red con detalle, dando a la protección y al control una nueva dimensión. Un conjunto de prestaciones de alta disponibilidad a nivel de hardware y del sistema mejoran drásticamente la continuidad del servicio permitiendo a los usuarios disfrutar de una conectividad fiable y de un mayor nivel de protección.

Equilibrio de carga UTM

Esta tecnología se diferencia por contar con el equilibrio de carga UTM, que consiste en combinar un motor Reassembly-Free Deep Packet Inspection y la clasificación de datos de alta velocidad con múltiples núcleos de seguridad, lo cual le permite inspeccionar en tiempo real aplicaciones, archivos y tráfico basado en contenido sin que ello repercuta significativamente en el rendimiento o en la escalabilidad del sistema. De esta forma es posible escanear y controlar las amenazas de las redes de clase empresarial con aplicaciones sensibles a la latencia y que requieren un gran ancho de banda. [WEB06]

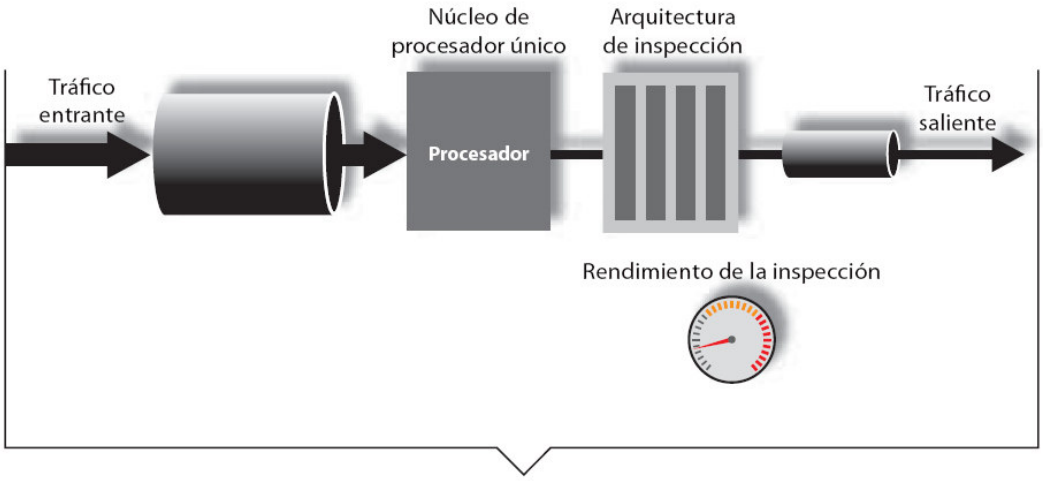


Figura 4.4 Tecnología de procesador único

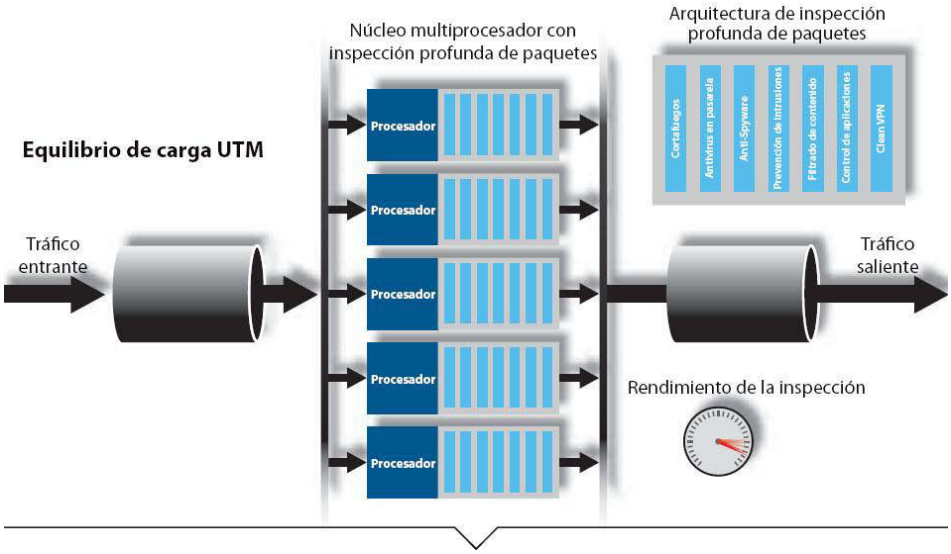


Figura 4.5 Arquitectura de tecnología multinucleo

2.2.2 Motor UTM

Esta tecnología proporciona un motor UTM escalable de de inspección a nivel de aplicación capaz de analizar archivos y contenidos de cualquier tamaño en tiempo real sin reensamblar los paquetes ni el contenido de las aplicaciones. Especialmente diseñado para aplicaciones en tiempo real y tráfico sensible a la latencia, este método de inspección ofrece un control y una inspección completos sin necesidad de recurrir a conexiones Proxy. Gracias a su diseño, este motor permite inspeccionar el tráfico de alta velocidad de forma más eficaz y segura y gozar de una mejor experiencia de usuario.

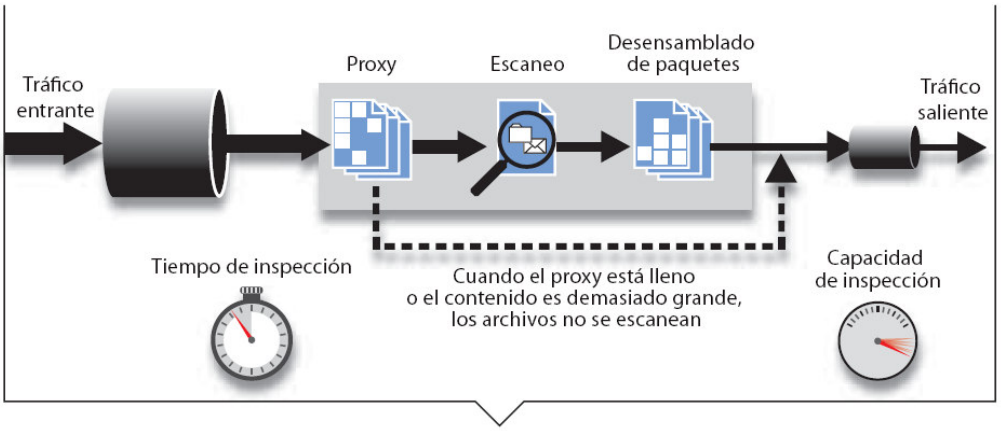


Figura 4.6 Proceso con ensamblado de paquetes

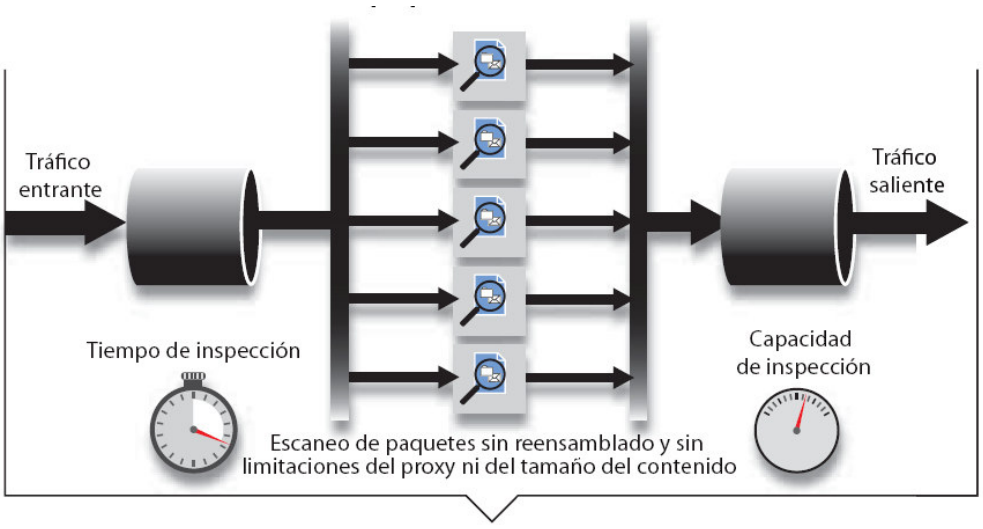


Figura 4.7 Proceso sin reensamblado de paquetes

3.1.3 Arquitectura de Tercera Tecnología

Esta tipo de tecnología se basa en proporcionar una seguridad inteligente distribuida en niveles, como se muestra en la Figura 4.8**,** donde es capaz de detectar y responder a las amenazas de la red en tiempo real, a la vez que es lo suficientemente flexible como para añadir rápidamente nuevos niveles de seguridad a medida que van surgiendo nuevas amenazas.

El motor de seguridad inteligente distribuida en niveles es el sistema nervioso central y se encarga de recopilar y evaluar la información de numerosos niveles, coordinar la mejor defensa y enviarle a usted esa información de manera proactiva.

La arquitectura de seguridad inteligente distribuida en niveles dispone de numerosas funciones de seguridad como, por ejemplo, Firewall con validación, prevención de intrusiones, redes VPN, filtrado a nivel de aplicaciones, bloqueo de correo no deseado, antivirus y servicios de filtrado de contenido. Gracias a la defensa en varios niveles integrada en una sola arquitectura, puede eliminar con eficacia diferentes tipos de tráfico hostil en cada nivel. Estos niveles trabajan en equipo para reforzarse unos a otros, por lo que cada uno tiene que procesar menos tareas. El resultado es una seguridad completa sin perjudicar el rendimiento de la red. [WEB07]

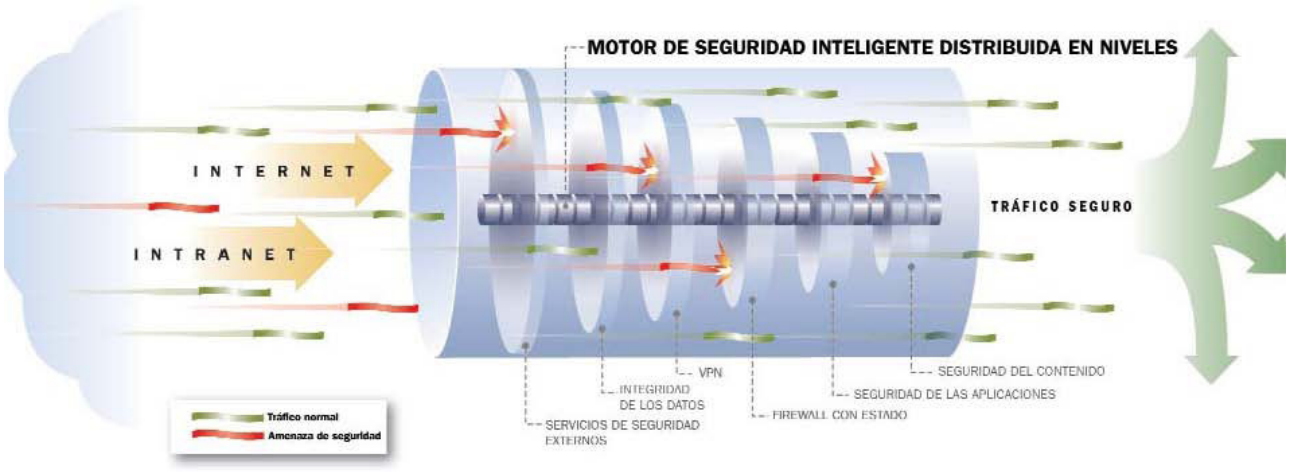


Figura 4.8 Motor de seguridad inteligente Distribuida en niveles

Figura 4.8, el motor de seguridad inteligente distribuida en niveles supervisa y dirige las actividades en múltiples niveles para obtenerla mejor protección y el rendimiento más elevado.

Protección Real para el Día Cero

La seguridad inteligente distribuida en niveles combina capacidades clave de seguridad capaces de defender su red contra distintas clases de ataques y de protegerla ante nuevas variantes, aún antes de que se hagan conocidas. Entre estas capacidades se cuentan: [WEB08]

- **La detección de anomalía de protocolo,** que bloquea el tráfico malicioso que no se ajusta a lo establecido en los protocolos estándares
- **El matching de patrones** marca y remueve archivos de alto riesgo del sistema, tales como .exe y scripts, virus, spywre y troyanos, luego de inspeccionar el paquete completo
- **El análisis de comportamiento** identifica y detiene el tráfico proveniente de hosts que muestran un comportamiento sospechoso, incluyendo ataques DoS y DDoS, escaneos de puertos y escaneos de direcciones.

La Ventana de Vulnerabilidad

La ventana de vulnerabilidad que se da entre el momento en que se lanza una nueva vulnerabilidad y el instante en que se desarrolla y se despliega la firma o el parche que la detecta.

Considerando la velocidad y la capacidad destructiva de los ataques actuales, aún unos pocos minutos sin protección pueden ser devastadores. La realidad es que en ocasiones, esta ventana dura horas y hasta semanas, convirtiéndose en una verdadera pesadilla para los gerentes de IT.

En el corazón de nuestras soluciones de seguridad, de este tipo de tecnología reside en una protección de Día Cero verdadera, que logra actuar antes de que la vulnerabilidad sea conocida.

CAPITULO IV:
IMPLEMENTACION TECNOLOGICA

CASO
MUNICIPALIDAD MIRAFLORES

4.1 Situación Actual

La Municipalidad de Miraflores es el órgano de Gobierno Local que representa y gestiona los intereses de los vecinos en la jurisdicción y promueve una gobernabilidad democrática.

La institución está conformada por 13 sucursales y una oficina principal (Palacio Municipal), donde en esta última reside el data center y por ende los servicios de red. En el anexo A se muestra el diagrama de la topología física de red de la Municipalidad de Miraflores y se describe los siguientes:

- En el recuadro de líneas punteadas etiquetado con el nombre de Oficina remotas, se muestra las oficina**s** remotas se encuentran interconectadas bajo la tecnológica de una red privada virtual sobre la plataforma de Conmutación de Multiprotocolo mediante etiquetas (**VPN/MPLS**).

- Se dispone de una zona DMZ (zona desmilitarizada), donde reside el servidor de Aplicaciones, servidor de dominio (DNS), servidor web y el servidor Webservice, las cuales serán accedidos por usuarios a través de internet e intranet.

- La zona MZ (zona militarizada), encontramos a los demás servidores que serán accedidos por usuarios de la red LAN. Siendo 14 servidor físicos y 9 servidores virtuales. Los servidores virtuales se encuentran implementados bajo la herramienta de Xen, de código abierto.

- La zona LAN, encontramos a las 500 usuarios distribuidos entre las oficinas remotas y la oficina central.

- La zona Testing, encontramos un servidor para realizar pruebas antes de ser puesta en producción.

- El servidor Firewall - Proxy bajo el sistema operativo de Software libre, Linux. Se implementó el servicios de firewall utilizando la herramienta de IPTABLES para el filtrado de paquetes en 4 zonas (LAN, TESTING,MZ y DMZ). El servicio de proxy cache con la herramienta Squid, que se encarga de restringir el acceso a páginas web de los usuarios que forman parte de la Zona LAN, este servicio cuenta con una cache de 20GB para ahorrar ancho de banda. También cuenta con una aplicación web, MYSAR, para monitorizar las páginas accedidas por los usuarios. Este servidor también dispone del servicio de DHCP, que se encarga de entregar IP dinámicamente en función de la dirección MAC del usuario.

4.1.1 Recursos Tecnológicos e Informáticos existentes:

- Enlaces a internet: 1 Enlace de 2Mbps.
- Cantidad de servidores en la DMZ: Posee (4) servidores en la DMZ.
- Posee (20) servidores físicos y 9 servidores virtuales. (BD ORACLE, CORREO, DOMINIO, Aplicaciones, etc.)
- 500 estaciones de trabajo distribuido en las 14 oficinas de la municipalidad.
- En la red de Datos convergen voz y dato.
- El servicio de Firewall- Proxy implementado sobre software libre, Linux.

4.2 Problemática

4.2.1 De Hardware

En la Municipalidad de Miraflores disponen de un servidor Firewall – Proxy basado en software libre, Linux, que posee las características de hardware: IBM xSeries 200 con disco duro de 20GB, memoria RAM de 512 MB, procesador Intel(R) Celeron 1.0 GHz y 4 interfaces de red. El hardware instalado no satisface las necesidades requeridas sobre todo en el procesador y la memoria RAM, el cual se proyectó una carga promedio de 200 usuarios pero con el crecimiento de la red alcanzó a los 400 usuarios por tanto el servidor se encuentra sobrecargado ocasionando una reducción de su performance y el deterioro del tiempo de respuesta día a día.

Toda la administración de la seguridad informática descansa en el servidor Firewall – Proxy, el equipo no está exento de sufrir fallas de hardware o de software ocasionando reducción de la disponibilidad del servicio y desprotección de la red.

4.2.2 De Software

El servidor firewall-Proxy bajo la plataforma de Linux, no se encuentra lo suficientemente actualizado por las limitaciones del hardware, cuenta con varios servicios de red, tales como: Firewall, proxy y DHCP, generando que algunos servicios como el caso del DHCP puede ser vulnerado así como la red entera a la que da protección.
La herramienta de filtrado de paquete sólo se realiza en la capa red es decir, no se analiza el contenido del paquete por tanto, no filtra los ataques por contenido.

Por otro lado, el servidor Firewall – Proxy, en caso de que sufra un ataque informático, que ocasiona parada del servicio, la red queda desprotegida y por ende afecta el funcionamiento de los demás servicios de red y en el peor de los casos se incremente el tiempo de inactividades de los servidores.

4.2.3 De la administración del Servicio

La administración el servidor de Firewall - Proxy es gestionado por terceros que origina los siguientes problemas:

- No se dispone de los privilegios para accesar y auditar el equipo y el servicio.
- Desconocimiento de la implementación de los servicios y su configuración de los servicios.
- Existe una dependencia muy fuerte con el proveedor y ante cualquier cambio, el más mínimo que sea, el administrador de red de la municipalidad debe de crear un ticket de atención, lo que genera el problema del tiempo de respuesta lento del proveedor frente a los ataques o vulnerabilidades.

4.3 Diseño de la Solución

Se debe de adquirir un equipo UTM especializado en la gestión de la seguridad informática de la red para poder resolver los problemas descritos. A continuación de justifica dicha adquisición en base a los problemas suscitados.

4.3.1 Justificación de la Solución

4.3.1.1 De Hardware

El equipo UTM dedicado dispone de características de hardware superiores al que se tiene. Las especificaciones técnicas: Procesador de 2.0 GHz tecnología RISC o CISC, disco duro de 80GB, memoria RAM de 1 GB, memoria Flash de 128 MB, 8 interfaces de red, una interfaz de alta disponibilidad de 1GbE (Gigabit Ethernet), una interface de consola para la administración del equipo y dos fuentes de alimentación redundantes.

El equipo permitirá soportar al menos 400 000 sesiones concurrentes y 18 000 nuevas sesiones por segundo.

Para aumentar la disponibilidad del equipo que gestiona la seguridad es necesario adquirir un equipo UTM adicional e implementar Clúster de Alta disponibilidad de tipo Activo – Pasivo.

4.3.1.2 De Software

Con la adquisición del equipo UTM se reducirá los tiempos de inactividad de los servicios de red, ya que utiliza una plataforma de Seguridad Multi-Capa, es decir el equipo dispone de servicios que en combinación de las funciones de Antivirus, filtrado de contenido, AntiSpam, Firewall e IDS/IPS brindará un mejor protección como también simplificará la gestión de la seguridad.

4.3.1.3 De la administración del Servicio

Con la adquisición del equipo UTM, el administrador de red tendrá los accesos necesarios para realizar modificaciones en la configuración del equipo por tanto se

reducirá la dependencia de terceros en la administración del equipo y control del mismo.

4.3.2 Especificaciones técnicas del equipo UTM

1. Poseer las funciones de Firewall, Traffic Shapping (Control de Tráfico), VPNs Antivirus Perimetral, Antispam Perimetral, IDS/IPS y Filtro de Contenidos dedicado para uso exclusivo de la protección del correo electrónico.

2. **Funcionalidades del Firewall:**
    - Soporte de al menos 400,000 sesiones concurrentes y 18,000 nuevas sesiones por segundo.
    - Un throughput (volumen de información) igual o mayor a 1.5 Gbps, considerando un promedio de 100,000 sesiones concurrentes a 160 kbps por sesión.
    - En el filtrado de paquetes debe utilizar la última tecnología denominada stateful inspection que permite brindar mejor rendimiento y seguridad.
    - Detector de Scanner de puertos.
    - El equipo deben tener una capacidad de manejar por lo menos 7,500 políticas distintas.

3. **Funcionalidades de VPN**
    - Soporte de VPN tipo site to site con un throughput igual o mayor a 600Mbps.
    - VPN compatibles con IPSEC Site to Site.
    - Soporte de clientes VPN remoto.

4. **Funcionalidades del IDS/IPS**
    - Soporte de un throughput de al menos de 780 Mbps.
    - La base de datos del IDS/IPS debe de actualizarse en forma automática.

5. **Funcionalidades del Antivirus**
    - Soporte de un throughput de al menos 155 Mbps.
    - La base de datos del antivirus debe de actualizarse en forma automática para garantizar el funcionamiento correcto de la seguridad perimetral.

6. **Funcionalidades del Filtro Web**
    - Soporte el Filtro Web por categorías, por URL y por contenido.
    - La base de datos del Filtro Web debe de actualizarse en forma automática.

7. **Funcionalidades del AntiSpam**
    - El equipo debe soportar al menos 800 estaciones de trabajo, los cuales reciben un promedio de 55 correos externos por hora, lo queda 44,000 correos y con una protección de 20%, el equipo debe controlar 53,000 correos por hora entre correos entrantes y correos salientes en inspección total.
    - Debe procesar todos los correos entrantes y salientes y manejar filtrado de políticas de acceso y contenido.
    - Debe contar con actualizaciones de reglas heurísticas dinámicas, filtrado de análisis de imágenes, filtrado de archivos PDF.

8. **Administración del Servicio**
    - Poseer consola de Administración modo lectura (reportes, estadísticas y gráficos).
    - Servicio de seguridad gestionada es 24x7.
    - El personal de la Municipalidad se encargará de la creación de las reglas, configuraciones en forma ilimitadas.

4.4 Alternativas de solución

Según las especificaciones técnicas del requerimiento de un dispositivo con Tecnología UTM, decidimos evaluar las propuestas de 3 marcas específicas, tomando en consideración el Cuadrante Mágico de Gartner.

El Cuadrante Mágico de Gartner es una representación gráfica de la situación del mercado de los dispositivos UTM en junio 2009 para medianas empresas como es el caso de la municipalidad de Miraflores. El gráfico está dividido en cuatro partes dónde se distribuyen las principales compañías en función de su tipología y la de sus productos:

El cuadrante de líderes (leaders): aquellos que tienen la mayor puntuación resultante al combinar su habilidad para ejecutar (lo bien que un vendedor vende y ofrece soporte a sus productos y servicios a nivel global) y el alcance de visión. Según la figura 4.4, tenemos a las compañías: Fortinet, SonicWall y WatchGuard.

El cuadrante de aspirantes (challengers): caracterizados por ofrecer buenas funcionalidades y un número considerable de instalaciones del producto, pero sin la visión de los líderes. Según la figura 4.4, tenemos a las compañías: Cisco y Juniper Network.

El cuadrante de visionarios (visionaries): estos pueden tener todas las capacidades que ha de ofrecer un ECM (Enterprise Content Management) de forma nativa, o mediante alianzas con otros socios, lo cual significa un fuerte impulso a la integración de programas y plataformas así como una habilidad para anticiparse a las necesidades del mercado que ellos no puedan cubrir. Según la figura 4.4, tenemos a las compañías: e IBM Internet Security Systems, Check Point Software Technologies, McAfee y Clavister.

Y **el cuadrante de nichos específicos (niche players):** enfocados a determinadas áreas de las tecnologías ECM, pero sin disponer de una suite completa. Según la figura 4.4, tenemos a las compañías: Astaro, NetASQ y Cyberoam.

Por lo expuesto precedentemente, decidimos seleccionar las tres marcas líderes que son: Fortinet, SonicWall y WatchGuard.

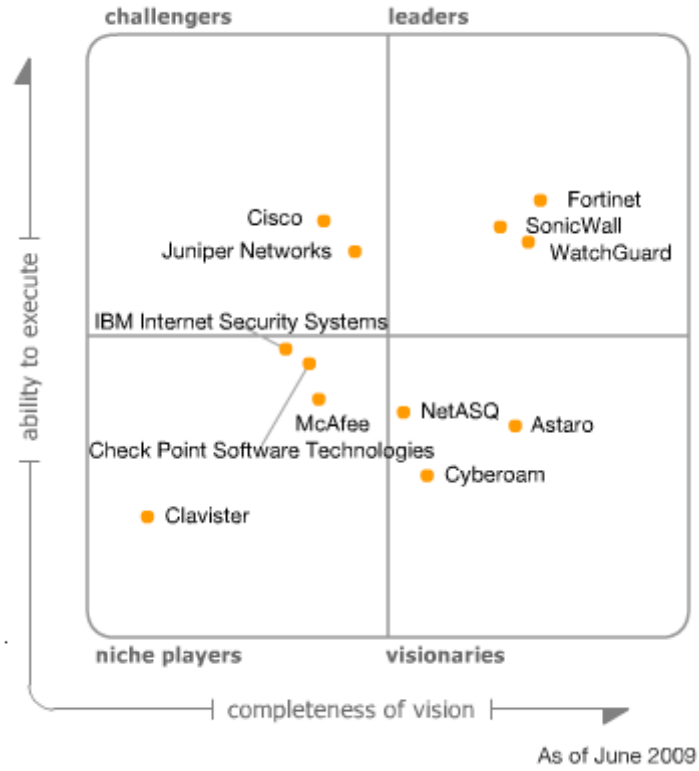


Figura4.9 Cuadrante Mágico de Gartner

Para la elección de un modelo correspondiente de cada fabricante nos basamos en los requerimientos de la Municipalidad de Miraflores que se determinó según las bases del concurso, donde requieren que el dispositivo UTM a seleccionar deberá soportar por lo mínimo: un Throughput de 2 Gbps para Firewall 500Mbps para VPN, asimismo un mínimo de 400 000 sesiones concurrentes. De acuerdo a estos criterios se seleccionó un dispositivo de cada fabricante que adapte a los requerimientos:

Alternativa 1: Fortigate 310B de la Compañía Fortinet.
Alternativa 2: SonicWALL NSA E6500 de la Compañía SonicWall.
Alternativa 3: Firebox® X8500e de la Compañía WatchGuard

Ahora describiremos las características más resaltantes de cada alternativa, ya que en el anexo C, se muestra la descripción técnica de cada equipo.

4.4.1 Fortigate 310B

Esta alternativa tiene es una poderosa combinación de software y hardware basada en el uso de "**Circuitos Integrados de Aplicación Específica**", conocidos por sus siglas en inglés como ASIC, a través de la cual es capaz de ofrecer el procesamiento y análisis del contenido del tráfico de la red sin que ello suponga ningún impacto en el rendimiento de las comunicaciones. La tecnología incluye el Procesador FortiASIC™ y el Sistema Operativo FortiOS™ los cuales forman el núcleo de los equipos FortiGate y son la base del alto rendimiento ofrecido por los equipos.

4.4.1.1 Características Resaltantes

4.4.1.1.1 FortiASIC™

La exclusiva arquitectura basada en ASIC empleada por los equipos Fortinet permite el análisis del contenido del tráfico en tiempo real, satisfaciendo todas las necesidades de protección a nivel de aplicación sin impactar en el rendimiento de la red.

El procesador FortiASIC™ posee múltiples características que hacen posible su alto rendimiento:

- Contiene un motor hardware que acelera el análisis de las cabeceras de cada paquete y del contenido ensamblado de los paquetes de una conexión, acelerando de este modo los procesos del motor del Firewall y del motor de IDS/IPS al ser capaz de identificar a velocidad de línea el flujo al que pertenece cada paquete.

- Posee un potente motor de comparación de firmas que permite comparar el contenido del tráfico de una sesión contra miles de patrones de firmas de virus, ataques de intrusión, u otros patrones sin comprometer el rendimiento de la red. Este motor de análisis reensambla los paquetes pertenecientes a un mismo mensaje en memoria, carga las firmas necesarias y realiza una búsqueda por comparación de patrones, todos estos procesos se realizan a nivel de hardware con la ganancia en velocidad que eso supone.

- El chip FortiASIC™ incluye también un motor de aceleración de cifrado que permite realizar cifrado y descifrado de alto rendimiento para el establecimiento de las Redes Privadas Virtuales o VPN.

- **Aceleración hardware para puertos de red (NP2).** El equipo FortiGate 3010B, tiene la propiedad de aceleración de hardware mediante puertos utilizando el NP2 (Network Processor). Mediante el uso de circuitos integrados de aplicación específica (ASIC) que dan servicio exclusivo a este tipo de puertos, se acelera la inspección de paquetes a nivel del propio puerto, liberando a la CPU e imprimiendo velocidad de línea a las transmisiones que los atraviesan, sea cual sea el tamaño de paquete utilizado. Además, existen varios módulos de expansión con formato AMC que incluyen puertos acelerados, esos módulos pueden contener 4 (ASM-FB4) u 8 (ASM-FB8) puertos GigabitEthernet con interfaz de cobre o 2 (ADM-XB2) puertos 10GigabitEthernet con interfaz SFP.

4.4.1.1.2 FortiOS™

El sistema operativo FortiOS™ fue diseñado con objeto de soportar funcionalidades de conmutación de alto rendimiento. El núcleo de FortiOS™ es un kernel dedicado, optimizado para procesamiento de paquetes y trabajo en tiempo real. Provee además de un interfaz homogéneo para cada una de las funcionalidades ofrecidas. Este sistema operativo funciona sobre diversos modelos de procesadores de propósito general, contando con biprocesadores en los equipos de gama alta. Esta flexibilidad permite emplear el mismo sistema operativo en todos los equipos FortiGate.

4.4.1.2 Componentes

Este equipo cuenta con servicios

- Firewall
- VPN con soporte de protocolos de IPSec, SSL y PPTP.
- Calidad de Servicio, gestiona el ancho de banda a nivel de políticas e interfaces.

- Antivirus basados en escaneo de firmas y escaneo heurístico. La base del conocimiento de vírus y El motor de escaneo se realiza automaticamente como manual.
- AntiSpam
- Filtrado de tráfico Web
- Protección contra intrusos (IPS), soporta ataques basados en Anomalía y firmas. La base de ataques y anomalias reconocidas y El motor de escaneo se realiza de manera automática o manual.
- Alta Disponibilidad, en modo Activo-Pasivo y Activo-Activo
- Optimización WAN
- Control del Aplicaciones

4.4.2 SonicWALL NSA E6500

Es la primera solución del mercado de Gestión unificada de amenazas (UTM) con arquitectura multinúcleo que ofrece Reassembly-Free Deep Packet Inspection™ de clase empresarial sin impactar significativamente en el rendimiento de la red. Los dispositivos E-Class NSA E6500 combinan un potente firewall de inspección profunda de paquetes con una tecnología de protección multicapa y prestaciones de alta disponibilidad.

Fueron diseñados para ser los dispositivos multifuncionales de gestión de amenazas de mayor rendimiento, escalabilidad y fiabilidad. Esto se debe a su arquitectura multinúcleo, que permite el procesamiento en paralelo garantizando una protección ultra rápida y un elevado nivel de escalabilidad. La prestación de la aplicación de Firewall se compone de un conjunto de herramientas de protección personalizables que permiten a los administradores controlar el tráfico de la red con detalle, dando a la protección y al control una nueva dimensión.

4.4.2.1 Características Resaltantes

4.4.2.1.1 Arquitectura multinúcleo de alto rendimiento

Está diseñada para ofrecer la más moderna tecnología de inspección profunda de paquetes y un control granular inteligente del tráfico de red en tiempo real, sin que el rendimiento de la red se vea afectado. Gracias a la labor simultánea de múltiples núcleos de procesamiento especializados, SonicWALL E-Class NSA es capaz de proporcionar un rendimiento efectivo ultra rápido. Al aprovechar la potencia de procesamiento de múltiples núcleos que funcionan al unísono, los dispositivos de esta serie mejoran enormemente el rendimiento y la capacidad de inspección simultánea, al tiempo que reducen los costes.

4.4.2.1.2 Equilibrio de carga UTM

Las soluciones que utilizan diversas tecnologías de protección, pero que solo cuentan con un único procesador central están extremadamente limitadas. Por ello, el equilibrio de carga UTM de SonicWALL combina un motor Reassembly-Free Deep Packet Inspection y de clasificación de datos de alta velocidad con múltiples núcleos de seguridad, lo cual le permite inspeccionar en tiempo real aplicaciones, archivos y tráfico basado en contenido sin que ello repercuta significativamente en el rendimiento o en la escalabilidad del sistema. De esta forma es posible escanear y controlar las amenazas de las redes de clase empresarial con aplicaciones sensibles a la latencia y que requieren un gran ancho de banda.

4.4.2.1.3 Motor UTM

El motor UTM de SonicWALL E-Class NSA es el primer motor escalable de inspección a nivel de aplicación capaz de analizar archivos y contenidos de cualquier tamaño en tiempo real sin reensamblar los paquetes ni el contenido de las aplicaciones. Especialmente diseñado para aplicaciones en tiempo real y tráfico sensible a la latencia, este método de inspección ofrece un control y una inspección completos sin necesidad de recurrir a conexiones Proxy. Gracias a su diseño, este motor permite inspeccionar el tráfico de alta velocidad de forma más eficaz y segura y gozar de una mejor experiencia de usuario.

4.4.2.2 Componentes

4.4.2.2.1 Servicios disponibles

- Application Firewall, abarca un conjunto de políticas granulares y configurables para aplicaciones que permite personalizar el control del acceso según usuarios de la red, aplicaciones, horarios o subredes IP.
- Calidad de servicio (QoS),
- VPNs
- Alta disponibilidad modo activa/activa y activo/pasivo.

4.4.2.2.2 Servicios Opcionales

- **Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention y Application Firewall.** Proporciona seguridad de red inteligente en tiempo real contra sofisticados ataques a nivel de aplicación y basados en contenido, como virus, spyware, gusanos, troyanos y vulnerabilidades de software.
- **Content Filtering Service.** Refuerza las políticas de protección y productividad mediante una arquitectura innovadora de clasificación. Gracias a una base de datos dinámica pueden bloquearse más de 56 categorías de contenido Web cuestionable.
- **ViewPoint** es una cómoda herramienta de informes basada en Web que proporciona una visión inmediata del rendimiento y la seguridad de la red. Gracias a la gran variedad de informes históricos basados en resúmenes y datos detallados, ViewPoint ayuda a organizaciones de todos los tamaños a supervisar el uso de Internet, a monitorear la seguridad de la red y a cumplir las leyes vigentes.
- **Soporte SonicWALL E-Class 24x7.**
- **Anti-Spam,** bloquea el spam, los ataques phishing y los mensajes infectados con virus en la pasarela. Gracias a este servicio, no es necesario redireccionar un registro MX ni enviar un correo electrónico a otro proveedor. Con un solo clic, el servicio se activa y comienza a bloquear el correo no deseado y a ahorrar ancho de banda valioso.

4.4.3 Firebox® XTM 810

Brinda una seguridad completa a las oficinas regionales pequeñas o medianas. Es la opción inteligente para las empresas que quieran una solución fuerte de seguridad de redes que ofrezca una manera fácil y accesible de extender la capacidad, el desempeño y las capacidades de networking a medida que el negocio cambia.

4.4.3.1 Características Resaltantes

La Arquitectura tiene incorporada Protección Real para el Día Cero

Las amenazas del Día Cero son ataques nuevos o desconocidos para los cuales aún no se escribió un parche ni una firma y la protección de Día Cero, por lo tanto, significa estar protegido ante las amenazas nuevas y desconocidas antes de que la vulnerabilidad sea descubierta y la vulnerabilidad haya sido creada y lanzada

El Intelligent Layered Security (ILS) en el dispositivo Firebox X brinda protección de Día Cero real. Asegura su red frente a amenazas nuevas y desconocidas antes de que la vulnerabilidad sea descubierta, creada y lanzada. Muchos proveedores sólo ofrecen protección basada en signatures. Estas soluciones reactivas dejan a sus usuarios expuestos a nuevos tipos de amenazas hasta que la vulnerabilidad se vuelve conocida, se escribe la signature correspondiente y se despliega la actualización para que los gerentes de IT la instalen. Entre estas capacidades se cuentan:

- **La detección de anomalía de protocolo,** que bloquea el tráfico malicioso que no se ajusta a lo establecido en los protocolos estándares.
- **El matching de patrones** marca y remueve archivos de alto riesgo del sistema, tales como .exe y scripts, virus, spywre y troyanos, luego de inspeccionar el paquete completo.

- **El análisis de comportamiento** identifica y detiene el tráfico proveniente de hosts que muestran un comportamiento sospechoso, incluyendo ataques DoS y DDoS, escaneos de puertos y escaneos de direcciones.

Fireware® XTM

Sistema operativo propietario que brinda versión Con las siguientes características: Enrutamiento Dinámico (BGP4, OSPF, RIP v1/2), basado en políticas; alta disponibilidad Activa/pasiva, activa/activa y con balance de carga, soporte de NAT, IP Virtual para balance de carga en el servidor y Soporte de SSL.

4.4.3.2 Componentes:

4.4.3.2.1 Servicios disponibles:

- Firewall, Inspección de paquetes stateful, inspección profunda de Aplicaciones,
- VPN soporte de los protocolos IPSec, SSL Y PPTP.
- Alta disponibilidad tipo activo-pasivo y activo-activo.

4.4.3.2.1 Servicios Opcionales:

4.4.3.2.1 WebBlocker es una suscripción de seguridad totalmente integrado al dispositivo Firebox X8500e. Permite que los administradores de TI para administrar el acceso web y contenido para una mayor seguridad y control de la navegación en la web. Bloquea los sitios maliciosos WebBlocker para mantener su red protegida de los contenidos Web peligrosos. Le ayuda a ahorrar ancho de banda de red, evitar la responsabilidad legal de contenidos inapropiados, y aumentar la productividad de los empleados mientras se protege la red contra ataques maliciosos de sitios web sin escrúpulos.

4.4.3.2.2 SpamBlocker proporciona en tiempo real la detección de spam para la protección inmediata de los brotes. Es la mejor solución en la industria en la distinción de comunicación legítimo del spam en tiempo real, el bloqueo de casi el 100% de los correos electrónicos no deseados. Spam es responsable de hasta el 95% del correo electrónico mundial y sigue siendo el método más común de propagación de virus. Se atasca el tráfico de red y conduce a los usuarios incautos a sitios Web maliciosos diseñados para robar información personal y la empresa.

4.4.3.2.3 Gateway AntiVirus (GatewayAV) es una suscripción de seguridad totalmente integrada para WatchGuard XTM aparatos. Se complementa con la inspección de aplicaciones contenido de la capa de la XTM para proporcionar protección en tiempo real contra virus, troyanos, gusanos, spyware y rogueware. Gateway AV analiza el tráfico en todos los principales protocolos, a través de firmas actualiza continuamente para detectar y bloquear todo tipo de malware.

4.4.3.2.4 Prevención de intrusiones (IPS) es una suscripción de seguridad totalmente integrado para todos los aparatos WatchGuard XTM. Trabaja en complementa con la inspección de aplicaciones contenido de la capa de la XTM para proporcionar protección en tiempo real contra las amenazas de la red, incluyendo spyware, inyecciones SQL, cross-site scripting, y desbordamientos de búfer.

4.5 Benchmarking de Las alternativas de solución

En la tabla 4.1 se detalla las principales características de cada modelo y las del servidor Firewall – Proxy bajo Linux que se encuentra en la cuarta, el cual puede agregar herramientas de Antivirus, Antispam, VPN, etc. instalando aplicativos adicionales que provean estas funcionalidades. Las soluciones bajo la plataforma de Linux ofrecen aplicaciones donde se beneficia con el licenciamiento libre y en algunos casos implican pago por su utilización. A continuación mostramos la tabla 4.1

RENDIMIENTO	FORTIGATE 310B	SonicWALL NSA E6500	Firebox® XTM 810	Fw Linux (*)
FIREWALL	8 Gbps	5 Gbps	3 Gbps	390 Mbps
VPN IPSEC	6 Gbps	2.5 Gbps	1 Gbps	No
ANTIVIRUS	160 Mbps	Licencia	Licencia	No
IPS	800 Mbps	Licencia	Licencia	No
SESIONES CONCURRENTES	600 000	750 000	500 000	25 000
NUEVAS SESIONES / SEGUNDO	20 000	20 000	No Publicado	9 000
INTERFACES	10 Base 10/100/1000	8 Base 10/100/1000	10 Base 10/100/1000	4 Base 10/100
PUERTO SERIAL	Si	Si	Si	Si
FILTRO DE CONTENIDO	Si	Licencia	Si	Si
CLUSTER HA	Activo/activo; Activo/Pasivo	Activo/activo; Activo/Pasivo	Activo/activo; Activo/Pasivo	No
CONTROL DE TRÁFICO	Si	Si	Si	Si
INSPECCION DE CONTENIDO SSL	Si	No	HTTPS Solamente	No
VPN SSL	Si	Licencia	Licencia	No
ANTISPAM	Si	Licencia	Licencia	No
VIRTUALIZACION	Si	No	No	No
MEMORIA	1 GB	1 GB	1 GB	512 MB
PROCESADOR	Intel(R) Celeron(R) CPU 2.00GHz	No Publicado	No Publicado	Intel Celeron CPU 1.0 GHz
FLASH	128 M	512 M	128 M	-
COSTO	$ 6 995	$ 17 995	$ 11525	-

Tabla 4.1 Benchmark de los dispositivos UTM

De la tabla 4.2 se pueda extraer los siguientes:

- El equipo **FORTIGATE 310B** presenta los más elevados rendimientos en Firewall y VPN IPSec de 8Gbps y 6 Gbps respectivamente.
- El equipo que soporta la mayor cantidad de sesiones concurrentes es el modelo **SonicWALL NSA E6500** alcanzando 750 000**.**
- Los equipos que presenta el control de aplicaciones son de la marca Fortinet y WatchGuard.

- La inspección de contenido SSL la marca WatchGuard sólo filtra el tipo de HTTPS mientras que el de Fortinet filtra además de SMTPS, POP3S e IMAPS.
- El único equipo que dispone de los servicios sin licencia de VPN SSL y ANTISPAM es el Fortinet 310B
- En cuanto a la Memoria Ram todos disponen de 1 GB pero en memoria Flash el que tiene mayor memoria es de SonyWall con 512 MB frente a los demás que solo tiene 128MB.
- En cuanto a procesador no se podría precisar si el de Fortinet es el mejor ya que en las demás marcas no se precisa esta información.

4.6 Selección de la Solución

Seleccionaremos el equipo que mejor se adapte o supere las requerimientos técnicos, por tanto decidimos elaborar la tabla 6.0, donde se especifican los factores de evaluación, los parámetros en las unidades que se puede medirse, el puntaje según el parámetro especificado, el máximo puntaje obtenido por dicha funcionalidad y mínimo puntaje obtenido por el mismo.

Asignamos un puntaje entre 0 y 30 puntos, según las funciones que se dispone. Las funcionalidades que tendremos en cuenta son: Rendimiento del Firewall, Rendimiento de VPN, Cantidad de Sesiones Concurrentes, Clúster de alta disponibilidad tipo activo-pasivo, y disponer los servicios (Filtrado de Contenido, Antivirus, Antispam, IDS/IPS y Control de tráfico).

Tabla 4.2 Factores de Evaluación

Funcionalidades	Parámetro		Puntajes	Max. Puntaje	Min. Puntaje
Rendimiento de Firewall	0 - 2 Gbps		10	30 puntos	10 puntos
	3 - 4 Gbps		20		
	5 Gbps a más		30		
Rendimiento de VPN	0 - 2 Gbps		10	30 puntos	10 puntos
	3 - 4 Gbps		20		
	5 Gbps a más		30		
Nº de sesiones concurentes por seg.	0 - 200000		0	30 puntos	0 puntos
	200001 - 400000		15		
	400001 - más		30		
Alta disponibilidad	Sólo activo - activo		0	30 puntos	0 puntos
	sólo activo - pasivo		15		
	Ambos modos		30		
Servicios disponibles	Filtro de contenido	Disponible	6	30 puntos	0 puntos
		Con licencia	0		
	Antivirus	Disponible	6		
		Con licencia	0		
	Antispam	Disponible	6		
		Con licencia	0		
	IDS/IPS	Disponible	6		
		Con licencia	0		
	Control del tráfico	Disponible	6		
		Con licencia	0		

Ahora realizamos una matriz que contemplen los parámetros descritos en la tabla 6.0 y las tres alternativas de solución con el objetivo de obtener la mejor alternativa de solución en base a los puntajes que lo hemos asignado.

Tabla 4.3 Evaluación de las alternativas de solución

Funcionalidades	Parámetro		Puntajes	Fortigate 310B	SonicWALL NSA E6500	Firebox® X8500e
Rendimiento de Firewall	0 - 2 Gbps		10	30	30	20
	3 - 4 Gbps		20			
	5 Gbps a más		30			
Rendimiento de VPN	0 - 2 Gbps		10	30	20	10
	2 - 4 Gbps		20			
	5 Gbps a más		30			
Nº de sesiones concurentes por seg.	0 - 200000		0	30	30	30
	200001 - 400000		15			
	400001 - más		30			
Alta disponibilidad	Sólo activo - activo		0	30	30	30
	sólo activo - pasivo		15			
	ambos modos		30			
Servicios disponibles	Filtro de contenido	Disponible	6	6	0	6
		Con licencia	0			
	antivirus	Disponible	6	6	0	0
		Con licencia	0			
	antispam	Disponible	6	6	0	0
		Con licencia	0			
	IDS/IPS	Disponible	6	6	0	0
		Con licencia	0			
	Control del tráfico	Disponible	6	6	6	6
		Con licencia	0			
TOTAL				**150**	**116**	**102**

En la tabla 4.3 se extrae los siguientes:

- La mejor alternativa es el Fortigate 310B de Fortinet, donde supera en toda las especificaciones técnicas requeridas, alcanzando el puntaje máximo de 150 puntos. Los servicios de Filtrado de Contenido, Antivirus, antispam, IDS/IPS y el control de

tráfico no requieren de licencia. Este equipo también goza de características adicionales como: Optimización WAN y el control de aplicaciones.

- La segunda alternativa a tener en cuenta sería SonyWall NSA E6500, ya que obtuvo un puntaje de 116 puntos, cabe señalar que esta alternativa cumple con todas las especificaciones técnicas requeridas pero con la excepción que los servicios de Filtro de contenido, antivirus, antispam e IDS/IPS se debe de paga una licencia por cada servicio que deseamos suscribirnos. En contraste con el equipo de Fortinet que tales servicios vienen listos para ser configurados y utilizados.

- Y por ultimo tenemos a la alternativa Firebox® X8500e, que obtuvo un puntaje de 102 puntos. Esta alternativa también cumple con las especificaciones técnicas pero igual que la alternativa anterior se debe adicionar un pago por licencia de cada servicios como: antivirus, antispam e IDS/IPS y con ello se incrementa el costo de adquisición del equipo.

A continuación mostramos algunas comparativas gráficas

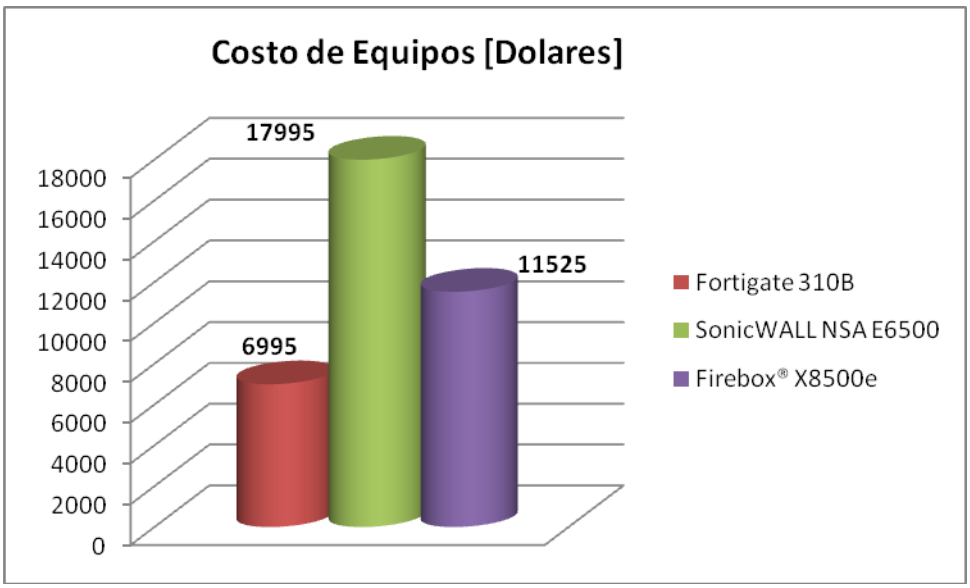


Figura 4.10 Cuadro estadístico del costo del equipo

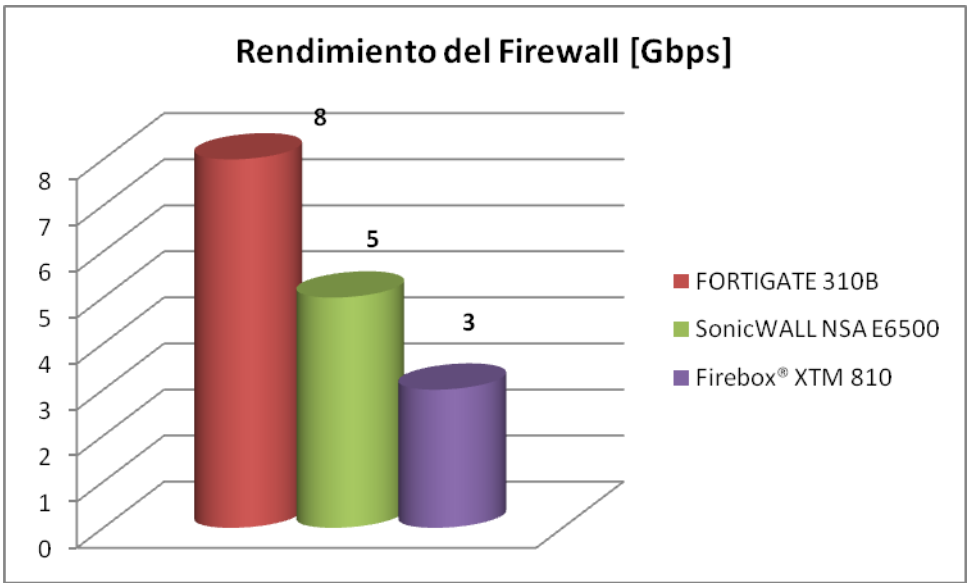


Figura 4.11 Cuadro estadístico del rendimiento del equipo

4.7 Inversión económica de la Solución

Según los requerimientos técnicos la alternativa seleccionada es Fortigate 310B. En la tabla 4.4 se muestra los precios de costo de cada alternativa, donde cabe señalar que en cuanto a la inversión económica también sería el equipo Fortigate 310B seleccionado con un precio de 6995 dólares.

La inversión económica de la implementación de la gestión de amenazas unificadas en la municipalidad de Miraflores con alta disponibilidad, se debe adquirir de 02 equipos Fortigate 310B, por lo tanto sería:

$$6995 \text{ X } 2 = 13990$$

Entonces la solución asciende a $ 13990 dólares.

Tabla 4.4 Precio de los equipos UTM

	Fortigate 310B	**SonicWALL NSA E6500**	**Firebox® X8500e**
INVERSION	$ 6 995	$ 17 995	$ 11525

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1. Los firewalls UTM centralizan la gestión y simplifican la administración de la seguridad informática.

2. La administración de la seguridad a través de los dispositivo UTM permite controlar las amenazas lógicas para reducir los tiempos de inactividad de los servicios de red, ya que proporcionan una seguridad distribuida en niveles y dispone de funciones como: Firewall, Antivirus, IDS/ IPS, Antispam y Web Filtering; que permiten eliminar con eficacia diferentes tipos de tráfico hostil en cada nivel. (Problema 1).

3. Se lograr aumentar la disponibilidad del equipo de UTM, utilizando dos dispositivos UTM y configurándolos en clúster de Alta Disponibilidad en Modo Activo/Pasivo, de esta manera el nodo Activo funcionará con las reglas y protección configurada, y en caso de desperfecto o avería el nodo Pasivo entrará en funcionamiento asegurando la continuidad de los servicios de red (Problema 2).

4. Se logra controlar el tráfico de la red mediante la implementación de equipos UTM a través de la herramienta de control de tráfico (Traffic Shaping) que permite realizar un mejor control del tráfico de las aplicaciones priorizando aquellos que son críticos asignándole ancho de banda acuerdo a su relevancia (Problema 3).

Del caso práctico, se concluye que el firewall UTM Fortigate 310B es el equipo que se adapta a las necesidades de la Municipalidad de Miraflores por las siguientes razones:

- Según las características recomendadas para la elección de un Firewall (Rendimiento y cantidad de conexiones concurrentes) posterior a la evaluación en los 3 equipos; es el equipo que presenta las mejores prestaciones bajo los parámetros de un equipo UTM.
- En base a la relación costo/beneficio, es el equipo que presenta una mayor relación costo/beneficio, dentro de las funciones solicitadas.

- Nuestra elección se basó en las características del equipo, que según en el cuadrante de Gartner, analistas de mercado tecnológico, pertenece a una empresa que fabrica soluciones del tipo UTM cumpliendo con los estándares y protocolos

5.2 Recomendaciones

1. La eficacia de la administración de la seguridad a través de equipos UTM dependerá y los usuarios de la red por tanto se recomiendan establecer políticas de seguridad que sean el soporte de la solución. A demás se debe concientizar a cada uno de los miembros de una organización sobre la importancia, sensibilidad de la información y servicios críticos (Conclusión 2).

2. Se recomienda mantener la disponibilidad de los recursos de red, adquiriendo equipos redundantes que puedan asegurar la continuidad en cuanto a la alimentación eléctrica hacia los componentes de la red local, los dispositivos que intercomunican a la red local hacia otros segmentos (internet y RPV). A demás se recomienda adquirir un enlace de contingencia. (Conclusión 3).

3. Se recomienda identificar las aplicaciones y los recursos críticos del negocio, para poder priorizar el tráfico de los servicios que se utilizan, de esta manera asegurarles velocidad, estabilidad y continuidad en sus comunicaciones. Caso contrario, a los servicios que no son críticos recomendamos limitar el uso del ancho de banda que utilizan, de esta manera no afectarán los demás servicios. (Conclusión 4).

4. La tecnología UTM es reciente y está evolucionando constantemente, con ello los recursos de hardware y software que utilizan se incrementan para poder proporcionar mayores prestaciones a los usuarios. Ha quedado demostrado a través de todas las organizaciones que la adoptaron, los beneficios tanto económicos como administrativos que proveen a las empresas. Por ello, con estos antecedentes y la tecnología, recomendamos utilizar un equipo con Plataforma de Gestión Amenazas Unificadas (UTM).

REFERENCIAS BIBLIOGRAFÍA

- **Bibliografía especializada**

[STA95] STALLINGS William, Network and Internet Security Principles and practice, New Jersy, 1995.

[ALV06] Álvaro Gómez Vieites, *Enciclopedia de la Seguridad Informática*, primera edición, 2006

[GUS97] Gustavo Miguel Aldegani, *Seguridad Informática*, Argentina 1997

[HUE02] HUERTA, Antonio Villalón. "Seguridad en Unix y redes". Versión 1.2 Digital – Open Publication License, 2002.

[CAR05] Carter Earl, CCSP IPS Exam Certification Guide, Cisco Press, 2005.

[RAN07] RANJBAR Amir S, CCNP ONT Official Exam Certification Guide, Cisco Press, 2007

[MICH00] Michael Hawkings y Floyd Piedad, "Alta Disponibilidad: Diseño, Técnicas y Procesos", 2000.

- **Revistas especializadas**

[BOR09] Lic. BORGHELLO Cristian, Cronología de los virus informáticos La historia del malware, Technical & Educational Manager de ESET para Latinoamérica, 2009

[GRA07a] GRAUE John William, Mecanismos de Calidad de Servicio, NexIT Specialist Nº 36 (p. 54), 2007.

[GRA07b] GRAUE John William, Manejando la congestión, NexIT Specialist Nº 37 (p. 38), 2007

- **Direcciones Electrónicas**

[WEB01] Henry Alexander Diaz Mongua, Hacking Ético: Taxonomía de un ataque, [consulta: 09 Marzo 2010], http://innovotech.byethost31.com/Archivos/pilodx1.pdf.

[WEB02]Ricardo Vargas de Basterra, [consulta: 09 Marzo 2010] http://www.iworld.com.mx/iw_Opinions_read.asp?IWID=64,

[WEB03] Polaxia Warez, [consulta: 09 Marzo 2010] http://polaxia.com/ataques-de-autenticacion-42607.0.html;wap2=

[WEB04] UNAM - CERT / DGSCA, [consulta: 10 Marzo 2010], http://www.seguridad.unam.mx/labsec/tuto/?id=135&ap=articulo&cabecera=2

[WEB05] Mambonet [consulta: 1 Abril 2010], http://www.mambonet.com/fabricantes/fortinet/Fortinet_Seguridad_Integral_en_Tiempo_Real.pdf.

[WEB06] Sonicwall, [consulta: 20 Abril 2010], http://www.sonicwall.com/downloads/DS_ES_NSA_Series_A4.pdf

[WEB07] Watchguard, [consulta: 21 Abril 2010], http://nitro2.com.ar/WatchGuard.pdf

[WEB08] Watchguard, [consulta: 27 Abril 2010], http://www.watchguard.com/docs/brochure/wg_utm_zeroday_es.pdf

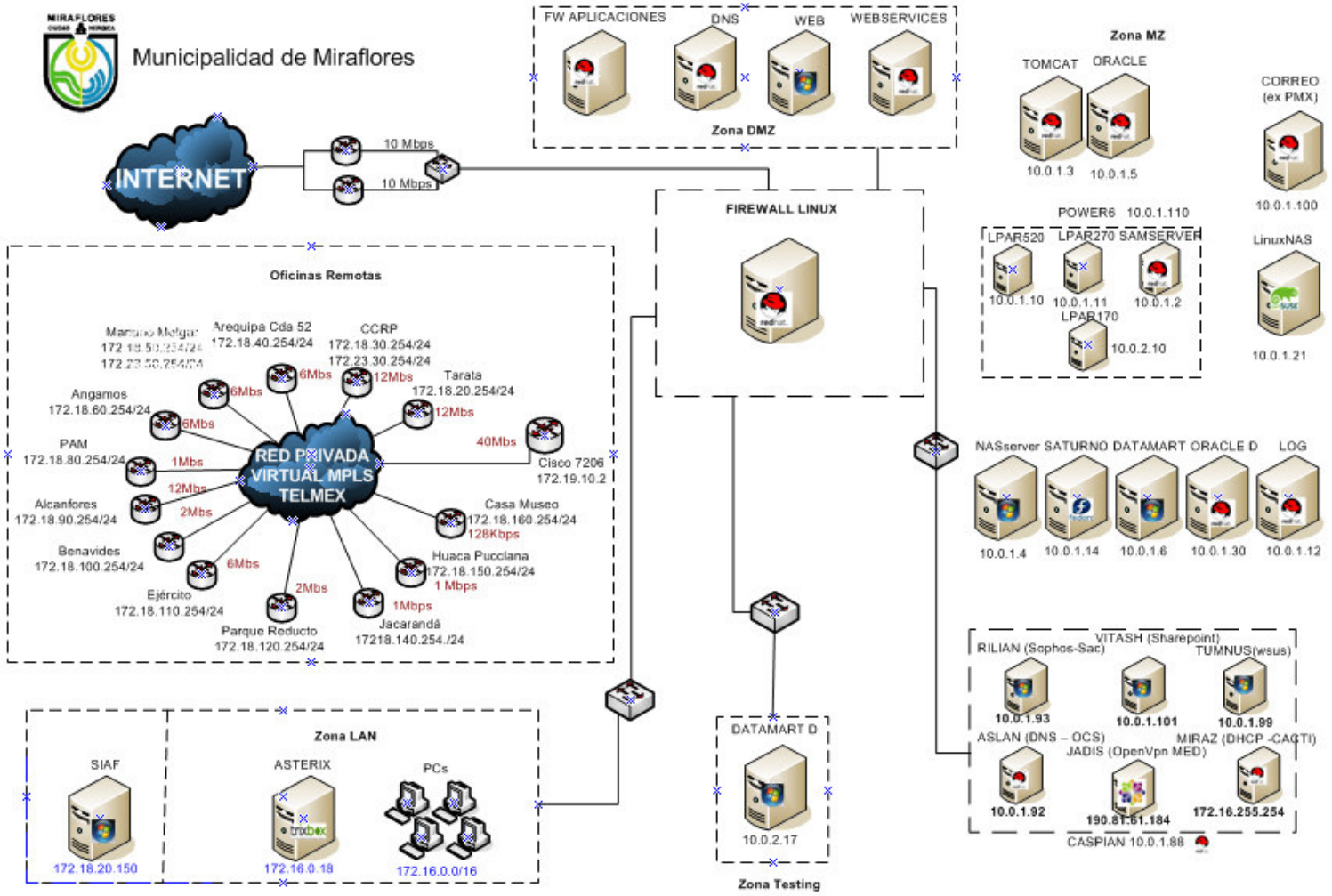
[WEB09] Sonicwall, [consulta: 20 Abril 2010],
http://www.sonicwall.com/downloads/DS_ES_E-Class_NSA_Series_A4.pdf

[WEB10] Watchguard, [consulta: 14 Abril 2010],
http://www.guardsite.com/XTM-810.asp

[WEB11] Fortinet, [consulta: 14 Abril 2010]
http://www.zen.co.uk/UserFiles/Documents/ZenFirewalls/FGT310B_DS.pdf

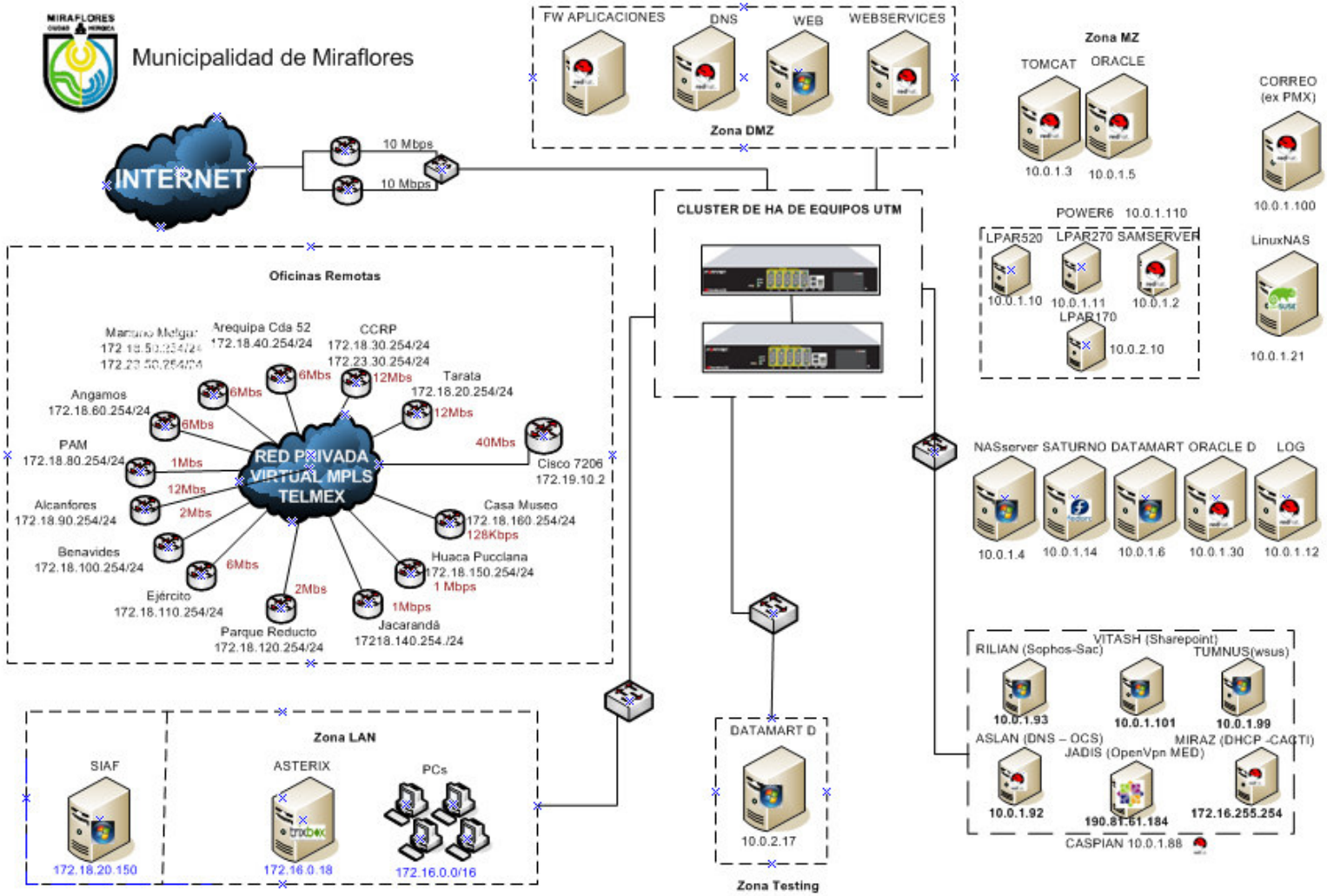
ANEXO A

TOPOLOGÍA DE LA INFRAESTRUCTURA FÍSICA DE LA MUNICIPALIDAD DE MIRAFLORES



ANEXO B

DISEÑO DE LA SOLUCION DE LA TOPOLOGIA FÍSICA DE LA MUNICIPALIDA DE MIRAFLORES



ANEXO C

ESPECIFICACIONES TÉCNICAS

1. SONICWALL NSA E6500 [WEB 09]

	NSA E5500	NSA E6500	NSA E7500
Firewall			
SonicOS Version		SonicOS Enhanced 5.6 (or higher)	
Stateful Throughput[1]	3.9 Gbps	5 Gbps	5.6 Gbps
GAV Performance[2]	1.0 Gbps	1.69 Gbps	1.84 Gbps
IPS Performance[2]	2.0 Gbps	2.3 Gbps	2.58 Gbps
UTM Performance[2]	850 Mbps	1.59 Gbps	1.7 Gbps
IMIX Performance[2]	1.1 Gbps	1.4 Gbps	1.6 Gbps
Maximum Connections[3]	750,000	1,000,000	1,500,000
Maximum UTM Connections	500,000	600,000	1,000,000
New Connections/Sec	15,000	20,000	25,000
Nodes Supported		Unrestricted	
Denial of Service Attack Prevention		22 classes of DoS, DDoS and scanning attacks	
SonicPoints Supported (Maximum)	96	128	128
VPN			
3DES/AES Throughput[4]	1.7 Gbps	2.7 Gbps	3 Gbps
Site-to-Site VPN Tunnels	4,000	6,000	10,000
Bundled Global VPN Client Licenses (Maximum)	2,000 (4,000)	2,000 (6,000)	2,000 (10,000)
Bundled SSL VPN Licenses (Maximum)	2 (50)	2 (50)	2 (50)
Virtual Assist Bundled (Maximum)	1 (25)	1 (25)	1 (25)
Encryption/Authentication/DH Groups	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1/DH Groups 1, 2, 5, 14		
Key Exchange	IKE, IKEv2, Manual Key, PKI (X.509), L2TP over IPSec		
Route-based VPN	Yes (OSPF, RIP)		
Certificate Support	Verisign, Thawte, Cybertrust, RSA Keon, Entrust, and Microsoft CA for SonicWALLto-SonicWALL VPN, SCEP		
Redundant VPN Gateway	Yes		
Global VPN Client Platforms Supported	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32-bit/64 bit, Windows 7		
SSL VPN Platforms Supported	Microsoft® Windows 2000 / XP / Vista 32/64-bit / Windows 7, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE		

2. FIREBOX X8500e [WEB 10]

XTM 810 Technical Specifications	
Throughput and Connections	
Firewall throughput*	3 Gbps
VPN throughput*	1 Gbps
XTM throughput*	850 Mbps
Interfaces 10/100/1000	10 copper
I/O interfaces	1 Serial, 2 USB DB-9
Nodes supported (LAN IPs)	Unrestricted
Concurrent sessions	500,000
VLANs (bridging, tagging, routed mode)	200
Local user database	400
VPN tunnels	
Branch Office VPN	1,000
Mobile VPN IPSec (incl/max)	600/2,000
Mobile VPN SSL	1,000
PPTP	50
Security:	
Firewall	Stateful packet inspection, deep packet inspection, proxy firewall
Application Proxies	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
Threat Protection	Blocks spyware, DoS attacks, fragmented packets, malformed packets, blended threats and more
VoIP	H.323. SIP, call setup & session security
Security subscriptions	WebBlocker, spamBlocker, Gateway AntiVirus, Intrusion Prevention Service (available in the Security Bundle)
VPN & Authentication	
Encryption	DES, 3DES, AES 128-, 192-, 256-bit
IPSec	SHA-1, MD5, IKE pre-shared Key, 3rd party cert

	import
SSL	Thin client, Web exchange
PPTP	Server & Passthrough
VPN Failover	Yes
Single Sign-On	Transparent Active Directory Auth.
XAUTH	Radius, LDAP, Windows Active Directory
Other User Authentication	VASCO, RSA SecurID, web-based, local
Networking	
Operating System	Fireware XTM Pro
IP Address Assignment	Static, DynDNS, PPPoE, DHCP (server, client, relay)
Routing	Static, dynamic (BGP4, OSPF, RIP v1/v2), policy-based
QoS	8 priority queues, diffserv, modified strict queuing
High Availability	Active/passive, active/active with load balancing
NAT	Static, dynamic, 1:1, IPSec NAT traversal, policy-based, virtual IP for server load balancing
Other Networking	Port independence, multi-WAN failover, multi-WAN load balancing, transparent/drop-in mode
Management	
Management Platform	WatchGuard System Manager (WSM) v.11 or higher
Alarms and Notifications	SNMP v2/v3, Email, Management System Alert
Server Support	Logging, Reporting, Quarantine, WebBlocker, Management
Web UI	Supports Windows, Mac, Linux, and Solaris OS
CLI	Includes direct connect and scripting
Hardware	
Product Dimensions	1.79"x16.9"x16.0" (44 x x 430 x 407 mm)
Shipping Dimensions	5.12" x 22.5" x 21.26" (130 x 566 x 540 mm)
Shipping Weight	19.5 lbs (8.8 Kg)
AC Power	100-240 VAC autosensing
Power Consumption	Max 215 Watt (734 BTU)
Rack Mountable	Yes (1U rack mount)
Certifications	
Security	ICSA, FIPS, EAL4 in progress
Safety	NRTL/C, CB
Hazardous Substance Compliance	WEEE, RoHS, REACH

3. FORTIGATE 310B [WEB 11]

FortiGate	310B Base Unit	310B with Optional ASM-FB4
Hardware Specifications		
Total 10/100/1000 Interfaces (Copper)	10	14
Configurable Ports	10	14
AMC Expansion Slot	1 Single Width	N/A
System Performance		
Firewall Throughput – Avg Size Packets (512 byte)	8 Gbps	12 Gbps
Firewall Throughput – Small Size Packets (64 byte)	8 Gbps	12 Gbps
VPN Throughput – 3DES	6 Gbps	9 Gbps
VPN Throughput – AES256	4 Gbps	6 Gbps
Antivirus Throughput*	160 Mbps	
IPS Throughput*	800 Mbps	
Dedicated IPSec VPN Tunnels	3,000	
Concurrent Sessions	500,000	
New Sessions/Sec	20,000	
Policies	8,000	
Unlimited User Licenses	Yes	

GLOSARIO DE TÉRMINOS

Access Control List: Lista de Control de Acceso o ACL, método para determinar los permisos de acceso apropiados a un determinado objeto.

ACM: Módulo avanzado de TCP/IP que permite conectar sus sistemas de seguridad con sus redes LAN/WAN, usando las conexiones de Internet e Intranet existentes.

ADM-XE2: Módulo de AMC, de doble ancho, que está compuesto por dos puertos de 10 Gbit XFP que permite acelerar el IPS.

Adware: Cualquier programa que automáticamente se ejecuta, muestra publicidad web al computador después de instalado el programa o mientras se está utilizando la aplicación.

Appliance: Dispositivo integrado de seguridad, son elementos robustos que integran tanto el hardware de conexión como un sólido sistema operativo, sobre el cual se colocan diversos bloques de seguridad.

ASIC: Circuito Integrado para Aplicaciones Específicas.

ASM-CE4: Módulo de AMC, de un solo ancho, está formado por 4 puertos 10/100/1000 Base-T y acelera IPS.

Backdoors: Es una secuencia especial dentro del código de programación mediante la cual el programador puede acceder o escapar de un programa en caso de emergencia o contingencia en algún problema, evadiendo los controles de acceso.

BitTorrent: Un programa de ordenador que permite a distintos ordenadores compartir ficheros a través de una red.

Black Hat: Es el nombre que se dan a las técnicas penalizables por los buscadores, esto quiere decir que los buscadores reconocen ciertas acciones que los webmasters realizan en sus websites para obtener mejores puestos dentro de los resultados naturales de los buscadores.

Chat: Designa una comunicación escrita realizada de manera instantánea a través de Internet entre dos o más personas

Cluster: Conjuntos o conglomerados de computadoras construidos mediante la utilización de componentes de hardware comunes y que se comportan como si fuesen una única computadora.

Connection flood: Todo servicio de Internet orientado a conexión tiene un límite máximo en el número de conexiones simultáneas que puede tolerar, cuando este límite es alcanzado no se admitirán nuevas conexiones.

Crackers: ES cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

DiffServ: Un método que intenta garantizar la calidad de servicio en redes de gran tamaño, como puede ser Internet.

DMZ: Zona desmilitarizada, red perimetral que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

DNS: Siglas en ingles de Domain Name System. Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado al internet o a una red privada. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

DoS: Siglas en inglés ***D**enial **o**f **S**ervice*. Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos

DDoS: Ataque de denegación de servicios distribuidos.

eDonkey: Es el nombre de una red de intercambio de archivos P2P, su nombre deriva del programa original creado para la misma. El nombre del cliente oficial es eDonkey2000.

Esteganografía: Disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

Exploits: significa en español, *explotar* o *aprovechar*. Es una pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico.

Failover: Procedimiento contra fallos de recursos en informática.

Fallback: Funciones especiales que después de un fallo en el sistema permiten completar las tareas pendientes.

Flooding: Jerga informática para designar un comportamiento abusivo de la red de comunicaciones, normalmente por la repetición desmesurada de algún mensaje en un corto espacio de tiempo.

Fragmentation Scanning: Técnica de escaneo. Consiste en hacer una división de los paquetes que enviamos, para no ser detectados por los packet filters y los firewall

FTP: sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.

Gateway: dispositivo de red que permite interconectar redes.

GNU/Linux: Términos empleados para referirse a la combinación del *kernel* libre similar a Unix denominado **Linux**, que es usado con herramientas de sistema GNU.

GNUTella: Proyecto de software distribuido para crear un protocolo de red de distribución de archivos entre pares, sin un servidor central.

Grayware: Es un tipo de programa maligno que se comportan de forma molesta o indeseada. También abarcan otros tipos de malwares (programas malignos) como espías, adwares, etc. Grayware no incluye virus o troyanos. Suelen afectar el rendimiento de la computadora.

Grey Hat: Personas de moral ambigua, que pueden ingresar sin autorización remotamente a redes privadas como también existes aquellos que depuran y arreglan errores en los sistemas.

Hackers: Gente apasionada por la seguridad informática.

Hardening: Proceso de asegurar un sistema reduciendo su entorno de vulnerabilidades, en otras palabras fortificar un sistema en contra de vulnerabilidades; un sistema totalmente seguro es aquél que se encuentra desconectado y aislado del exterior. Una situación así se antoja irreal.

Heartbeat: El software de clúster sobre alta disponibilidad de los equipos físicos, gracias a la técnica de heartbeat.

H.323: Es una recomendación del ITU-T (International Telecommunication Union), que define los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red.

ICMP: Siglas en ingles de Internet Control Message Protocol. Es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).

ICQ: Software cliente de mensajería instantánea y el primero de su tipo en ser ampliamente utilizado en Internet, mediante el cual es posible chatear y enviar mensajes instantáneos a otros usuarios conectados a la red de ICQ.

IDS/ IPS: Sistema de detección de intrusión y Sistema de prevención de intrusión

IMAP: Siglas en ingles de Internet Message Access Protocol, protocolo de red de acceso a mensajes electrónicos almacenados en un servidor.

Intserv: Significa Servicios Integrados .Modelo de servicio de Calidad de servicio

Ip Hijacking: Secuestro de una conexión TCP/IP por ejemplo durante una sesión Telnet permitiendo a un atacante inyectar comandos o realizar un DoS durante dicha sesión.

iPhone: Teléfono inteligente multimedia con conexión a internet, pantalla táctil y una interfaz de hardware minimalista.

iPod: Es una marca de reproductores multimedia portátiles diseñados y comercializados por Apple Inc.

IPSec VPN: Red Privada Virtual implementado bajo el protocolo de comunicación IPSec.

IRC: Siglas en ingles de Internet Relay Chat. Es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas.

Jitter: Cambio o variación en cuanto a la cantidad de latencia entre paquetes de datos que se reciben.

KaZaa: Aplicación que permite el intercambio de archivos de música, video, texto, imágenes, y aplicaciones, de forma muy amigable.

Kernel: Es la base de un sistema operativo que permite a este interactuar con el hardware.

Linux: Es un sistema operativo, una gran software que controla un computador. Es parecido a Microsoft Windows, pero completamente libre.

Man-in-the-Middle: es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

NAT: Siglas en ingles de Network Address Translation o Traducción de Dirección de Red. Estándar para la utilización de una o más direcciones IP para conectar varias computadoras a una red (especialmente Internet).

PAT: Siglas en ingles de Port Address Translation - Traducción de Direcciones por Puerto. Se dispone de una sola IP pública y se traduce cualquier dirección privada a ESA IP pública.

PBX: Central Telefónica Digital. Sistema telefónico dentro de una organización que maneja las llamadas entre sus usuarios en líneas locales mientras permite que entre todos los usuarios compartan un número determinado de líneas telefónicas externas.

Phishing: El "phishing" es una modalidad de estafa diseñada con la finalidad de robarle la identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

POP3: (Post Office Protocol 3 - Protocolo 3 de Correo). Es un protocolo estándar para recibir mensajes de e-mail. Los mensajes de e-mails enviados a un servidor, son almacenados por el servidor pop3. Cuando el usuario se conecta al mismo (sabiendo la dirección POP3, el nombre de usuario y la contraseña), puede descargar los ficheros.

Pop-up: son ventanas emergentes.

QoS: Calidad de Servicio (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de video o voz.

RAM: (Random Access Memory - Memoria de acceso aleatorio). Tipo de memoria donde la computadora guarda información para que pueda ser procesada más rápidamente. En la memoria RAM se almacena toda información que está siendo usada en el momento.

Router: ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un router es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

RPC: Siglas en ingles de Remote Procedure Call - Llamada a Procedimiento Remoto. Protocolo que permite a una aplicación en una computadora ejecutar código en otra remota sin tener que preocuparse por la comunicación entre ambas. Las RPC suelen utilizarse en los programas tipo cliente/servidor.

RST: Es un código usado para describir la calidad de las transmisiones de radio

RTSP: Siglas en ingles de Real Time Streaming Protocol - El protocolo de flujo de datos en tiempo real. Establece y controla uno o muchos flujos sincronizados de datos, ya sean de audio o de video. El RTSP actúa como un mando a distancia mediante la red para servidores multimedia.

Script Kiddies: Denominado también script bunny, script kitty. En terminología hacker, es una palabra despectiva usada para designar a aquellos crackers sin experiencia que utilizan programas desarrollados por otros para atacar sistemas o dañar sitios web.

Shoulder Surfing: Consiste en espiar físicamente a los usuarios, para obtener generalmente claves de acceso al sistema.

SIP: Protocolo de Inicialización de Sesiones. Protocolo de aplicación que pretende ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario, donde hay componentes como video, voz, juegos online, realidad virtual y mensajería instantánea.

Skype: Es una aplicación que permite hacer llamadas telefónicas por internet. Llamar a otros usuarios del servicio es gratuito, como así también a líneas gratuitas, pero sí tienen cargos otras líneas y teléfonos celulares.

SMTP: (Simple Mail Transfer Protocol - Protocolo de Transferencia Simple de Correo). Protocolo estándar para enviar e-mails.

SMTP Simple Message Transfer Protocol)

Smurf: Es un ataque de denegación de servicio. se basa en paquetes dirigidos a la dirección de Broadcast de una red.

Sniffing: Un programa de sniffing permite a alguien escuchar las conversaciones entre ordenadores que fluyen por las redes.

Snooping: El snooping tiene como objetivo obtener información de una red a la que están conectados sin modificarla, similar al sniffing (packet sniffer). Además de interceptar el tráfico de red, el atacante accede a documentos, mensajes de e-mail y otra información privada guardada en el sistema, guardando en la mayoría de los casos esta información en su equipo.

SPAM: correo basura o sms basura a los mensajes no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor

Spoofing: El spoof tradicional es cuando los 'atacantes' falsean el origen de los paquetes haciendo que la víctima piense que estos son de un host de confianza o autorizado para saltar un firewall o que la víctimas no nos detecten.

SSH: Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente

SSL VPN: Acceso remoto seguro a recursos críticos desde prácticamente cualquier punto, como equipos de escritorio, portátiles y dispositivos PDA.

Stateful Inspection: Es parte de la arquitectura de los firewalls. Consiste en examinar de manera dinámica los paquetes de datos que llegan al firewall.

SYN: Son paquetes que son enviados o recibidos para establecer una "sincronizacion" entre 2 host o un lugar remoto o sitio de internet remoto hacia tu pc

Syn flood: Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Tcp Connect Scanning: Esta es la forma mas popular de escaneo TCP y consiste básicamente en usar la llamada a sistema connect() del sistema operativo, si se logra establecer la conexión con el puerto de la otra computadora entonces este puerto esta abierto.

Threat Agent: Agentes de la amenaza

Throughput: Es el fenómeno que produce cambios, es el mecanismo de conversión de las entradas en salidas o resultados. Generalmente es representado como la caja negra, en la que entran los insumos y salen cosas diferentes, que son los productos.

TIC: tecnologías de la información y la comunicación

Traffic Shapping: Intenta controlar el tráfico en redes de ordenadores para así lograr optimizar o garantizar el rendimiento, baja latencia, y/o un ancho de banda determinado retrasando paquetes

Trashing: Es la técnica de recuperar o investigar sobre información que ha sido abandonada o eliminada.

UDP: Siglas en ingles de User Datagram Protocol - Protocolo de Datagrama de Usuario). Protocolo abierto, no orientado a la conexión (como el TCP) y por lo que no establece un diálogo previo entre las dos partes, ni tampoco mecanismos de detección de errores.

URL: Es una dirección que permite acceder a un archivo o recurso como ser páginas html, php, asp, o archivos gif, jpg, etc. Se trata de una cadena de caracteres que identifica cada recurso disponible en la WWW.

UTM: siglas en ingles de Unified Threat Management dispositivo que permite la gestión unificada de amenazas;

VLAN: Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

VoIP: (Voice over Internet Protocol, voz sobre internet). Enrutamiento de conversaciones de voz sobre internet u otra red basada en el protocolo IP.

VPN: de siglas en ingles Virtual Private Network. Tecnología de redes que permite la extensión de una red de área local sobre una red pública o no controlada (como internet).

VPN / MPLS: Implementación de una Red Privada Virtual utilizando tecnología MPLS.

Web Filtering Es una solución integrada que cuenta con protección contra el software espía con filtrado de contenido. Hace cumplir las políticas de uso de Internet bloqueando el acceso a sitios Web y aplicaciones de Internet que no estén relacionadas con el negocio y de forma fácil y por completo elimina el software espía y otras formas de software maligno de su organización

Webmail: Es un servicio online que permite crear cuentas de e-mail que pueden ser revisadas a través de la web.

White Hat: Son los hackers que no buscan el daño ajeno, o, por lo menos, utilizan el hacking como defensa.